

SmartSwitch 7000 User's Guide

CABLETRON
systems

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Virus Disclaimer

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © 1998 by Cabletron Systems, Inc. All rights reserved.

Printed in the United States of America.

Order Number: 9031895-02 July 1998

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

Cabletron Systems, SPECTRUM, BRIM, DNI, FNB, INA, Integrated Network Architecture, LANVIEW, LANVIEW Secure, Multi Media Access Center, MiniMMAC, and TRMM are registered trademarks, and **Bridge/Router Interface Modules, BRIM-A100, CRBRIM-W/E, CRXMIM, CXRMIM, Desktop Network Interface, Distributed LAN Monitoring, Distributed Network Server, DLM, DNSMIM, E1000, E2000, E3000, EFDMMIM, EMM-E6, EMME, EPIM, EPIM-3PS, EPIM-A, EPIM-C, EPIM-F1, EPIM-F2, EPIM-F3, EPIM-T, EPIM-T1, EPIM-X, ESXMIM, ETSMIM, ETWMIM, FDCMIM-04, FDCMIM-08, FDMIM, FDMIM-04, Flexible Network Bus, FOMIM, FORMIM, HubSTACK, IRBM, IRM, IRM-2, IRM-3, Media Interface Module, MicroMMAC, MIM, MMAC, MMAC-3, MMAC-3FNB, MMAC-5, MMAC-5FNB, MMAC-8, MMAC-8FNB, MMAC-M8FNB, MMAC-Plus, MRX, MRXI, MRXI-24, MultiChannel, NB20E, NB25E, NB30, NB35, NBR-220/420/620, RMIM, SecureFast Switch, SecureFast Packet Switching, SFS, SFPS, SPECTRUM Element Manager, SPECTRUM for Open Systems, SPIM-A, SPIM-C, SPIM-F1, SPIM-F2, SPIM-T, SPIM-T1, TPMIM, TPMIM-22, TPMIM-T1, TPRMIM, TPRMIM-36, TPT-T, TRBMIM, TRMM-2, TRMMIM, and TRXI** are trademarks of Cabletron Systems, Inc.

AppleTalk, Apple, Macintosh, and TokenTalk are registered trademarks; and Apple Remote Access and EtherTalk are trademarks of Apple Computer, Inc.

SmartBoost is a trademark of American Power Conversion

ST is a registered trademark and C++ is a trademark of AT&T

Banyan and VINES are registered trademarks of Banyan Systems, Inc.

cisco, ciscoSystems, and AGS+ are registered trademarks; and cBus, cisco Router, CRM, IGS, and MGS are trademarks of cisco Systems, Inc.

GatorBox is a registered trademark; and GatorMail, GatorMIM, GatorPrint, GatorShare, GatorStar, GatorStar GX-M, and XGator are trademarks of Cayman Systems, Inc.

CompuServe is a registered trademark of CompuServe Incorporated

X Window System is a trademark of Consortium, Inc.

CTERM, DECnet, and ULTRIX are registered trademarks; and DEC, DEC C++, DECnet-DOS, DECstation, VAX DOCUMENT, VMA, and VT are trademarks of Digital Equipment Corporation

Fore Systems, ForeRunner, and ForeRunner ASX-100 are trademarks of Fore Systems, Inc.

PC/TCP is a registered trademark of FTP Software, Inc.

HP OpenView is a registered trademark of Hewlett-Packard, Inc.

AIX, IBM, OS/2, NetView, and PS/2 are registered trademarks; and AT, Micro Channel, PC, PC-DOS, PC/XT, Personal Computer AT, Operating System/2, Personal System/2, RISC System/6000, and Workplace Shell are trademarks of International Business Machines Corporation

i960 microprocessor is a registered trademark; and Intel and Multichannel are trademarks of Intel Corporation

Microsoft, MS-DOS, and Windows are registered trademarks of Microsoft Corporation

Chameleon, ChameleonNFS, Chameleon 32, IPX/link, and NEWT are trademarks of NETMANAGE, Inc.

NetWare and Novell are registered trademarks; and Internetwork Packet Exchange (IPX), IPX, and Network File System (NFS) are trademarks of Novell, Inc.

Motif and MS are registered trademarks; and Open Software Foundation, OSF, OSF/1, and OSF/Motif are trademarks of The Open Software Foundation, Inc.

Silicon Graphics and IRIS are registered trademarks; and Indigo and IRIX are trademarks of Silicon Graphics, Inc.

NFS, PC-NFS, SPARC, Sun Microsystems, and Sun Workstation are registered trademarks; and OpenWindows, SPARCstation, SPARCstation IPC, SPARCstation IPX, Sun, Sun-2, Sun-3, Sun-4, Sun386i, SunNet, SunOS, SunSPARC, and SunView are trademarks of Sun Microsystems, Inc.

OPEN LOOK and UNIX are registered trademarks of Unix System Laboratories, Inc.

Ethernet, NS, Xerox Network Systems and XNS are trademarks of Xerox Corporation

ANNEX, ANNEX-II, ANNEX-IIe, ANNEX-3, ANNEX-802.5, MICRO-ANNEX-XL, and MICRO-ANNEX-ELS are trademarks of Xylogics, Inc.

MAXserver and Xyplex are trademarks of Xyplex, Inc.

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.
 - (b) This computer software may be:
 - (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;
 - (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;
 - (3) Reproduced for safekeeping (archives) or backup purposes;
 - (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;
 - (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and
 - (6) Used or copied for use in or transferred to a replacement computer.
 - (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.
 - (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.
 - (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

Chapter 1 Introduction

Using the SmartSwitch 7000 User's Guide.....	1-3
Related Manuals.....	1-4
Software Conventions	1-4
Common Window Fields.....	1-4
Using the Mouse	1-6
Using Window Buttons.....	1-7
Getting Help	1-7
Using On-line Help.....	1-7
Getting Help from the Cabletron Systems Global Call Center	1-8
SmartSwitch 7000 Firmware.....	1-8

Chapter 2 The SmartSwitch 7000 Chassis View

Viewing Chassis Information.....	2-2
Front Panel Information.....	2-4
Menu Structure.....	2-5
Port Status Displays.....	2-10
Selecting a Port Status View.....	2-10
Port Status Color Codes.....	2-12
The Chassis Manager Window	2-12
Viewing Hardware Types	2-13
Device Type	2-14
Module Type.....	2-14
Viewing I/F Summary Information.....	2-15
Interface Performance Statistics/Bar Graphs.....	2-16
Viewing Interface Detail	2-18
Making Sense of Detail Statistics.....	2-20
Viewing FDDI Statistics	2-20
Setting the FDDI Statistics Polling Interval	2-21
Using the Find Source Address Feature	2-22
Managing the Hub	2-23
Configuring Ports	2-23
Configuring Ethernet and FDDI Ports.....	2-23
Configuring Fast Ethernet Ports.....	2-24
Setting the Desired Operational Mode.....	2-27
Configuring the COM Ports.....	2-29
Setting the Device Date and Time	2-31
Enabling and Disabling Ports	2-32

Chapter 3 Statistics

Accessing the Statistics Window	3-1
RMON Statistics	3-2
Viewing Total, Delta, and Accumulated Statistics.....	3-5
Printing Statistics	3-6
Interface Statistics.....	3-7

Chapter 4 Alarm Configuration

About RMON Alarms and Events	4-1
Basic Alarm Configuration	4-2
Accessing the Basic Alarm Configuration Window	4-3
Viewing Alarm Status	4-4
Creating and Editing a Basic Alarm	4-6
Disabling a Basic Alarm	4-8
Viewing the Basic Alarm Log	4-9
Advanced Alarm Configuration	4-10
Accessing the RMON Advanced Alarm/Event List.....	4-10
Creating and Editing an Advanced Alarm.....	4-13
Creating and Editing an Event.....	4-19
Adding Actions to an Event	4-23
Deleting an Alarm, Event, or Action	4-25
Viewing an Advanced Alarm Event Log.....	4-25
How Rising and Falling Thresholds Work	4-26

Chapter 5 FDDI Management

Configuration.....	5-2
Connection Policy	5-6
Station List.....	5-9
Stations Panel.....	5-10
Performance	5-11

Chapter 6 ATM Configuration

Accessing the ATM Connections Window	6-1
Configuring Connections	6-4
Adding a New Connection.....	6-4
Deleting a Connection	6-5

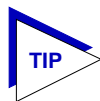
Index

Introduction

How to use this guide; related guides; software conventions; getting help; Smart Switch 7000 firmware versions

Welcome to the *SPECTRUM Element Manager for the SmartSwitch 7000 User's Guide*. We have designed this guide to serve as a simple reference for using SPECTRUM Element Manager for the Smartswitch 7000 family of hubs.

SPECTRUM Element Manager provides management support for all three models in the SmartSwitch 7000 family. The **7C03 MMAC SmartSwitch** functions as a chassis within a chassis; residing in an MMAC-series hub, it occupies two module slots and provides three slots of its own — one for the 7X00 SmartSwitch Control Module, and two for its own family of Network Interface Modules, or NIMs. The **7C04 Workgroup SmartSwitch** is a stand-alone chassis that offers four slots: one for the controller, and three for NIMs. The **7C04-R Workgroup SmartSwitch** supplies all the features of the 7C04 along with the additional fault tolerance provided by a pair of redundant load-sharing power supplies and a removable fan tray. The 7C04-R can also accept the new double-wide NIM modules (in slots 3 and 4) for additional front panel connectivity.



The 7C03 MMAC SmartSwitch chassis provides no network connection to the MMAC backplane (from which it draws only power). If you wish to connect one or more networks from the MMAC chassis to the SmartSwitch chassis, you must do so via the front panel ports available on both the MMAC MIMs and the SmartSwitch NIMs.

At the heart of each SmartSwitch 7000 hub is its 7X00 SmartSwitch Control Module, which supervises access to the switching backplane and performs all forwarding, filtering, and connection management functions; a variety of NIM modules provide connectivity for FDDI, Ethernet, Fast Ethernet, and ATM networks. NIM modules currently available include:

- The **7E03-24**, a single-slot Ethernet module that provides 24 ports via two RJ71 connectors.
- The **7E02-24**, a double-wide Ethernet module for the 7C04-R which provides 24 ports via RJ45 connectors.
- The **7F06-02**, which provides connectivity for two FDDI ring networks via its two front-panel FPIM slots; FPIM modules that support both multi-mode fiber and single-mode fiber (both with MIC connectors) and both shielded and unshielded twisted pair (with RJ45 connectors) are available.
- The **7H02-06**, which provides six Fast Ethernet connections — the first via a Fast Ethernet Port Interface Module slot, and an additional five via built-in Category 5 UTP RJ45 connectors. Two Fast Ethernet port modules are available: the FE-100FX, which provides a single multi-mode fiber port with an SC connector; and the FE-100TX, with a single Category 5 UTP RJ45 connector.
- The **7H02-12**, a double-wide module which provides 12 Fast Ethernet connections — the first via a Fast Ethernet Port Interface Module slot, and another 11 via built-in UTP RJ45s.
- The **7H06-02** Fast Ethernet uplink module, which provides two Fast Ethernet connections via Fast Ethernet Port Interface Module slots.
- The **7A06-01**, which provides a redundant ATM uplink connection via two front panel ATM Port Interface Module slots. Available APIMs provide connectivity for all standard ATM speeds and media types.

The available modules provide your SmartSwitch hub with key mission-critical features such as redundant links, alarm thresholding, and full error breakdown; with at least one Ethernet or Fast Ethernet module installed in the chassis, per-port RMON support is also provided. By default, the 7X00 performs traditional switching (or bridging); depending on the version of firmware you have installed, the 7X00 module can also be configured to perform Cabletron's SecureFast switching.



Not all released firmware versions support the ability to select SecureFast switching; check your hardware manuals to see if your version of firmware supports this feature. Currently, the toggle from traditional bridging to SecureFast switching is performed via Local Management; see your Local Management documentation for details.

Note that because the 7C03, 7C04, and 7C04-R provide the same functionality and support the same family of NIM modules (with the exception of the double-wide modules, which can be installed only in a 7C04-R), they will be referred to collectively throughout this manual as the SmartSwitch 7000. Where there are

differences, however, each device will be named separately, as necessary. Note, too, that the information displayed in many of the windows will differ slightly depending upon which type of device is being managed; however, only a single screen will be shown unless significant differences in functionality exist.

Using the SmartSwitch 7000 User's Guide

Each chapter in this guide describes one major functionality or a collection of several smaller functionalities of the SmartSwitch 7000 hubs and their installed modules. This guide contains information about software functions which are accessed directly from the device icon; for information about management functions which are accessed via the SPECTRUM Element Manager platform, consult the *User's Guide* and the *Tools Guide*.

Chapter 1, **Introduction**, provides a list of related documentation, describes certain software conventions, and shows you how to contact Cabletron Systems' Global Call Center. A brief description of each of the SmartSwitch 7000 chassis models and the NIMs they support is also provided.

Chapter 2, **The SmartSwitch 7000 Chassis View**, describes the visual display of the SmartSwitch 7000 chassis and explains how to use the mouse within the Chassis View; the operation of several chassis-level management functions — such as changing the chassis display, enabling and disabling ports, setting device date and time, and configuring ports — is also described here.

Chapter 3, **Statistics**, describes the two statistics views available at the interface level: FDDI and ATM interfaces provide MIB-II Interface statistics; Ethernet and Fast Ethernet interfaces supply RMON statistics.

Chapter 4, **Alarm Configuration**, provides instructions for using both the Basic and Advanced alarm applications to configure both alarms and the events that notify you that an alarm condition has occurred. The ability to automatically initiate a SET or a series of SETs in response to an alarm — functionality provided by Cabletron's proprietary Actions MIB — is also described.

Chapter 5, **FDDI Management**, describes the Configuration, Connection Policy, Station List, and Performance selections available from the FDDI menu.

Chapter 6, **ATM Configuration**, describes how to configure Permanent Virtual Circuits (PVCs) for any installed ATM modules.

We assume that you have a general working knowledge of Ethernet IEEE 802.3, Fast Ethernet, ATM, and FDDI type data communications networks and their physical layer components, and that you are familiar with general bridging and switching concepts.

Related Manuals

The SmartSwitch 7000 user's guide is only part of a complete document set designed to provide comprehensive information about the features available to you through SPECTRUM Element Manager. Other guides which supply important information related to managing the SmartSwitch 7000 include:

Cabletron Systems' *SPECTRUM Element Manager User's Guide*

Cabletron Systems' *SPECTRUM Element Manager Tools Guide*

Cabletron Systems' *SPECTRUM Element Manager Remote Administration Tools User's Guide*

Cabletron Systems' *SPECTRUM Element Manager Remote Monitoring (RMON) User's Guide*

Cabletron Systems' *SPECTRUM Element Manager Alarm and Event Handling User's Guide*

Cabletron Systems' *Network Troubleshooting Guide*

Microsoft Corporation's *Microsoft Windows User's Guide*

For more information about the capabilities of the SmartSwitch 7000 hub and its available modules, consult the appropriate hardware documentation.

Software Conventions

SPECTRUM Element Manager's device user interface contains a number of elements which are common to most windows and which operate the same regardless of which window they appear in. A brief description of some of the most common elements appears below; note that the information provided here is not repeated in the descriptions of specific windows and/or functions.

Common Window Fields

Similar descriptive information is displayed in boxes at the top of most device-specific windows in SPECTRUM Element Manager, as illustrated in [Figure 1-1](#) (following page).

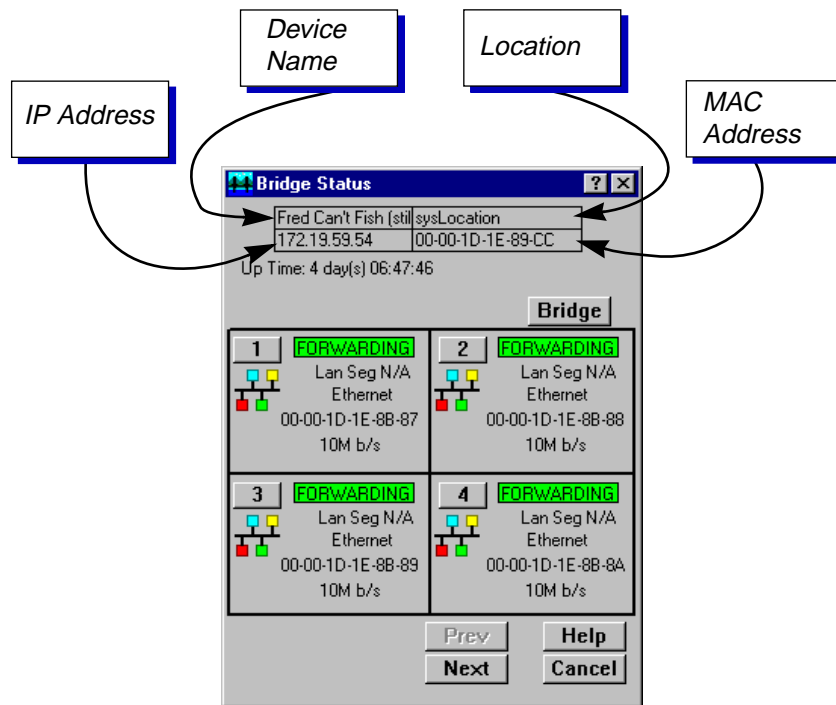


Figure 1-1. Sample Window Showing Group Boxes

Device Name

Displays the user-defined name of the device. The device name can be changed via the System Group window; see the *Generic SNMP User's Guide* for details.

IP Address

Displays the device's IP (Internet Protocol) Address; this will be the IP address used to define the device icon. The IP address is assigned via Local Management to the 7X00 Control Module's internal Host interface; it cannot be changed via SPECTRUM Element Manager. Note that although each interface in the SmartSwitch 7000 hub has its own MAC, or physical, address, only a single IP address is assigned.

Location

Displays the user-defined location of the device. The location is entered through the System Group window; see the *Generic SNMP User's Guide* for details.

MAC Address

Displays the manufacturer-set MAC address associated with the IP address used to define the device icon; this will be the MAC address assigned to the 7X00 Control Module's internal Host interface. Note that each interface in the SmartSwitch 7000 chassis has its own MAC address; these addresses are factory-set and cannot be altered.

Using the Mouse

This document assumes you are using a Windows-compatible mouse with two buttons; if you are using a three button mouse, you should ignore the operation of the middle button when following procedures in this document. Procedures within the SPECTRUM Element Manager document set refer to these buttons as follows:

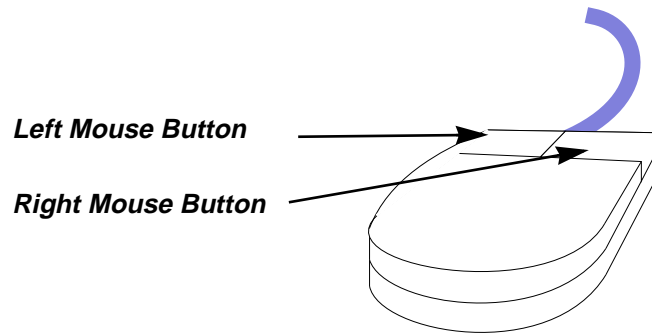


Figure 1-2. Mouse Buttons

For many mouse operations, this document assumes that the left (primary) mouse button is to be used, and references to activating a menu or button will not include instructions about which mouse button to use.

However, in instances in which right (secondary) mouse button functionality is available, instructions will explicitly refer to **right** mouse button usage. Also, in situations where you may be switching between mouse buttons in the same area or window, instructions may also explicitly refer to both **left** and **right** mouse buttons.

Instructions to perform a mouse operation include the following terms:

- **Pointing** means to position the mouse cursor over an area without pressing either mouse button.
- **Clicking** means to position the mouse pointer over the indicated target, then press and release the appropriate mouse button. This is most commonly used to select or activate objects, such as menus or buttons.
- **Double-clicking** means to position the mouse pointer over the indicated target, then press and release the mouse button two times in rapid succession. This is commonly used to activate an object's default operation, such as opening a window from an icon. Note that there is a distinction made between "click twice" and "double-click," since "click twice" implies a slower motion.
- **Pressing** means to position the mouse pointer over the indicated target, then press and hold the mouse button until the described action is completed. It is often a pre-cursor to Drag operations.

- **Dragging** means to move the mouse pointer across the screen while holding the mouse button down. It is often used for drag-and-drop operations to copy information from one window of the screen into another, and to highlight editable text.

Using Window Buttons

The **Cancel** button that appears at the bottom of most windows allows you to exit a window and terminate any unsaved changes you have made. You may also have to use this button to close a window after you have made any necessary changes and set them by clicking on an **OK**, **Set**, or **Apply** button.

An **OK**, **Set**, or **Apply** button appears in windows that have configurable values; it allows you to confirm and SET changes you have made to those values. In some windows, you may have to use this button to confirm each individual set; in other windows, you can set several values at once and confirm the sets with one click on the button.

The **Help** button brings up a Help text box with information specific to the current window. For more information concerning Help buttons, see **Getting Help**, [page 1-7](#).

The command buttons, for example **Bridge**, call up a menu listing the windows, screens, or commands available for that topic.

Any menu topic followed by ... (three dots) — for example **Statistics...** — calls up a window or screen associated with that topic.

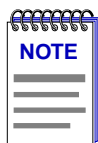
Getting Help


This section describes two different methods of getting help for questions or concerns you may have while using SPECTRUM Element Manager.

Using On-line Help

You can use the **Help** buttons to obtain information specific to a particular window. When you click on a Help button, a window will appear which contains context-sensitive on-screen documentation that will assist you in the use of the windows and their associated command and menu options. Note that if a Help button is grayed out, on-line help has not yet been implemented for the associated window.

From the **Help** menu accessed from the Chassis View window menu bar, you can access on-line Help specific to the Chassis View window, as well as bring up the Chassis Manager window for reference. Refer to Chapter 2 for information on the Chassis View and Chassis Manager windows.



All of the online help windows use the standard Microsoft Windows help facility. If you are unfamiliar with this feature of Windows, you can select **Help** from the  **Start** menu, or **Help** —> **How to Use Help** from the primary SPECTRUM Element Manager window, or consult your Microsoft Windows product **User's Guide**.

Getting Help from the Cabletron Systems Global Call Center

If you need technical support related to SPECTRUM Element Manager, or if you have any questions, comments, or suggestions related to this manual or any of our products, please feel free to contact the Cabletron Systems Global Call Center via one of the following methods:

By phone:	(603) 332-9400 <i>24 hours a day, 365 days a year</i>
By mail:	Cabletron Systems, Inc. PO Box 5005 Rochester, NH 03866-5005
By Internet mail:	support@ctron.com
FTP:	ftp.ctron.com (134.141.197.25)
<i>Login</i>	anonymous
<i>Password</i>	your email address
By BBS:	(603) 335-3358
Modem Setting	8N1: 8 data bits, 1 stop bit, No parity

For additional information about Cabletron Systems products, visit our World Wide Web site: <http://www.cabletron.com/>. For technical support, select **Service and Support**.

SmartSwitch 7000 Firmware

SPECTRUM Element Manager support for the SmartSwitch 7000 has been tested against released firmware version 1.05.09 for the 7X00 Controller Module, and pre-release version 1.04.07 for the 7A06-01 NIM (the only NIM which currently has independent firmware); if you have an earlier version of firmware and experience problems, contact Cabletron Systems Global Call Center for upgrade information.

The SmartSwitch 7000 Chassis View

Information displayed in the Chassis View window; the logical chassis view; the Chassis Manager window; hub management functions

The SmartSwitch 7000 Chassis View window is the main screen that immediately informs you of the current configuration of your SmartSwitch chassis via a graphical display of the chassis front panel. The default Logical View shows the boards installed in your SmartSwitch according to the physical slots they occupy, and displays the condition of individual interfaces on those boards. The Chassis View window serves as a single point of access to all other SmartSwitch 7000 windows and screens, which are discussed at length in the following chapters.

To access the SmartSwitch 7000 Chassis View window, use one of the following options:


1. In any map, list, or tree view, double-click on the SmartSwitch 7000 you wish to manage;

or

1. In any map, list, or tree view, click the **left** mouse button once to select the SmartSwitch 7000 you wish to manage.



Figure 2-1. The SmartSwitch 7000 Icon

2. Select **Manage—>Node** from the primary window menu bar, or select the Manage Node  toolbar button.

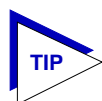
or


1. In any map, list, or tree view, click the **right** mouse button once to select the SmartSwitch 7000 you wish to manage.
2. On the resulting menu, click to select **Manage**.

Viewing Chassis Information

The SmartSwitch 7000 Chassis View window (Figure 2-2, following page) provides a graphic representation of the SmartSwitch 7000 hub and its installed modules, including a color-coded port display which immediately informs you of the current configuration and status of all the port interfaces installed in the SmartSwitch chassis. Note that the Chassis View window for the 7C03 MMAC SmartSwitch shows the modules in a vertical position, as they are actually installed in the MMAC chassis; the Chassis View for the 7C04 and 7C04-R Workgroup SmartSwitches show the modules in a horizontal position. Note, too, that the slots in the 7C03 chassis are numbered from left to right; in the 7C04 chassis, they're numbered top to bottom; and on the 7C04-R chassis, they're numbered bottom to top.

By clicking in designated areas of the chassis graphical display (as detailed later in this chapter), or by using the menu bar at the top of the Chassis View window, you can access all of the menus that lead to more detailed windows.



When you move the mouse cursor over a management “hot spot,” the cursor icon will change into a hand symbol  to indicate that clicking in the current location will bring up a management option.



Note that up to 24 ports can be displayed simultaneously on a module. If a module has a higher port density than 24 ports, arrows will appear at the top and bottom (or left and right, as appropriate) of the port stack so that you can scroll through the remaining ports.

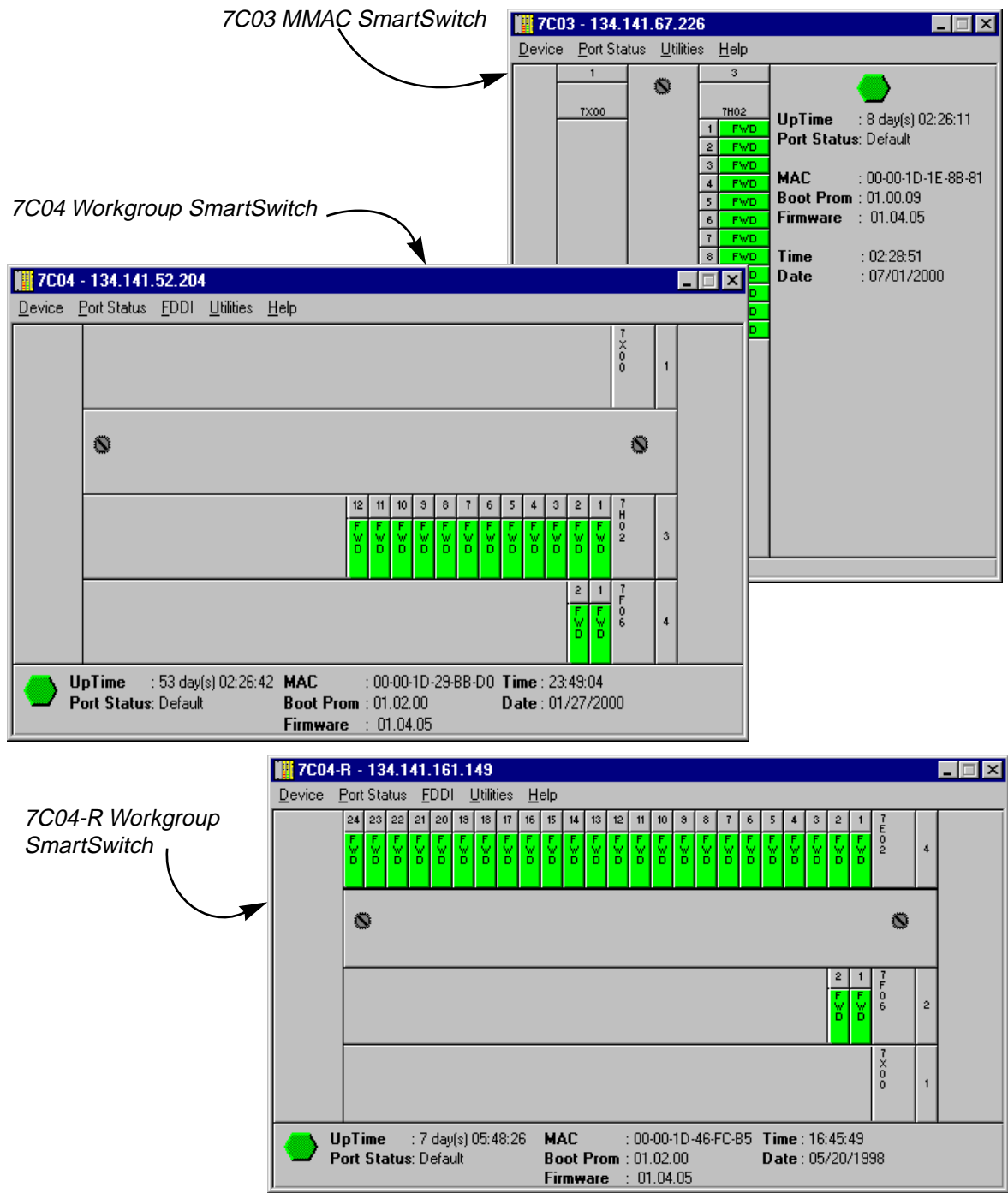


Figure 2-2. SmartSwitch Chassis View Windows

Front Panel Information

In addition to the main interface display, the Chassis View window provides the following device information:

IP

The Chassis View window title displays the device's IP (Internet Protocol) Address; this will be the IP address used to define the device icon. The IP address is assigned via Local Management to the 7X00 Control Module's internal Host interface; it cannot be changed via SPECTRUM Element Manager. Note that although each interface in the SmartSwitch 7000 hub has its own MAC, or physical, address, only a single IP address is assigned.

Connection Status



This color-coded area indicates the current state of communication between SPECTRUM Element Manager and the SmartSwitch 7000.

- **Green** indicates the SmartSwitch 7000 is responding to device polls (valid connection).
- **Magenta** indicates that the SmartSwitch 7000 is in a temporary stand-by mode while it responds to a physical change in the hub (such as when a board is inserted); note that board and port menus are inactive during this stand-by state.
- **Blue** indicates an unknown contact status; polling has not yet been established with the SmartSwitch 7000.
- **Red** indicates the SmartSwitch 7000 is not responding to device polls (device is off line, or device polling has failed across the network for some other reason).

UpTime

The amount of time, in a days hh/mm/ss format, that the SmartSwitch 7000 has been running since the last start-up.

Port Status

Indicates the Port Status display selection currently in effect. The default port status view is bridge status; if you have not changed the port status selection since launching the Chassis View window, this field will display **Default**. For more information about changing the port status display, see [page 2-10](#).

MAC

Displays the manufacturer-set MAC address associated with the IP address used to define the device icon; again, this will be the MAC address assigned to the 7X00 Control Module's internal Host interface. Note that each interface in the SmartSwitch 7000 chassis has its own MAC address; these addresses are factory-set and cannot be altered.

Boot Prom

The revision of BOOT PROM installed in the 7X00 Control Module.

Firmware

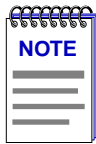
The revision of device firmware stored in the 7X00 Control Module's FLASH PROMs.

Time

The current time, in a 24-hour hh:mm:ss format, set in the 7X00 Control Module's internal clock.

Date

The current date, in an mm/dd/yyyy format, set in the 7X00 Control Module's internal clock.



You can set the date and time by using the *Edit Device Date* and *Edit Device Time* options on the Device menu; see *Setting the Device Date and Time*, [page 2-31](#), for details.

In accordance with Year 2000 compliance requirements, SPECTRUM Element Manager now displays and allows you to set all dates with four-digit year values.

Menu Structure

By clicking on various areas of the SmartSwitch 7000 Chassis View display, you can access menus with device-, board-, and port-level options, as well as utility applications which apply to the device. The following illustration displays the menu structure and indicates how to use the mouse to access the various menus:

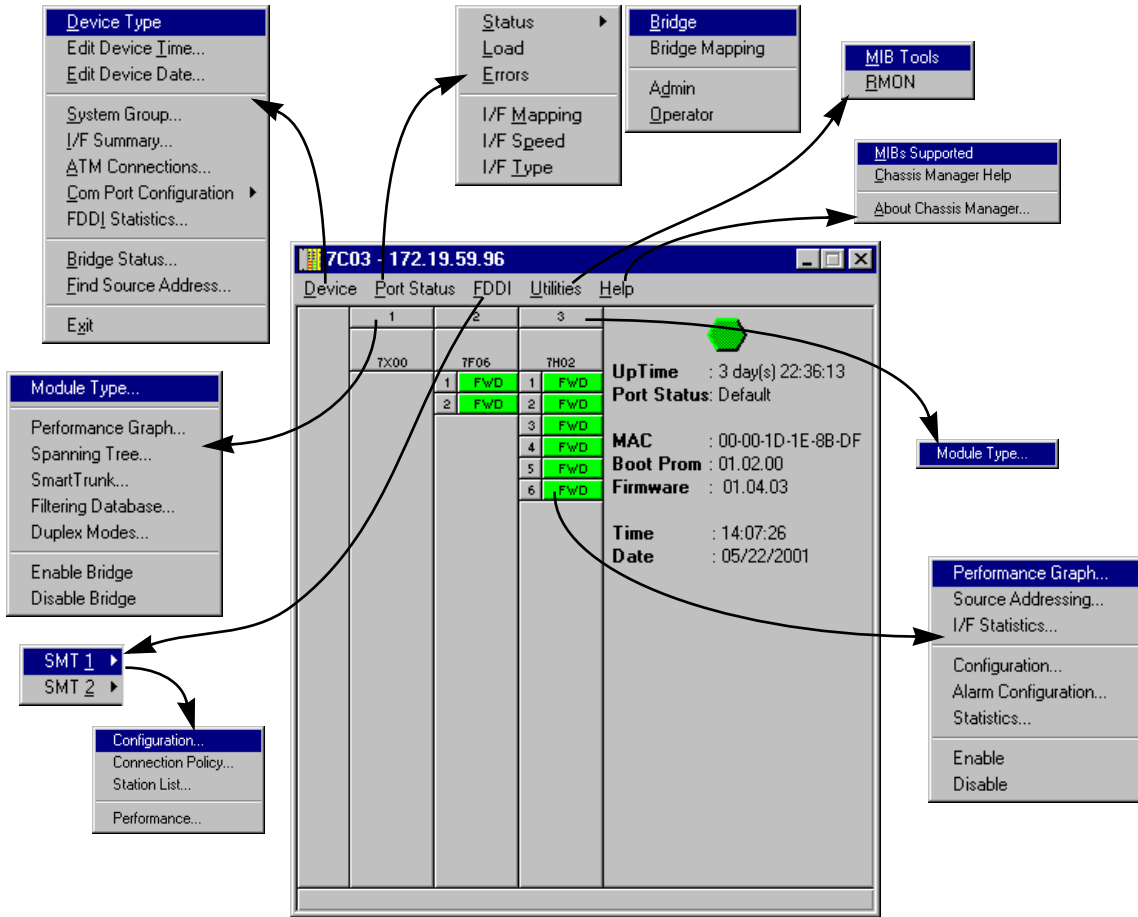


Figure 2-3. SmartSwitch 7000 Chassis View Menu Structure

The Device Menu

From the Device Menu at the Chassis View window menu bar, you can access the following selections:

- **Device Type...**, which displays a window containing a description of the device being modeled: 7C03 - MMAC SmartSwitch, 7C04 - WorkGroup SmartSwitch, or 7C04-R WorkGroup SmartSwitch.
- **Edit Device Time** and **Edit Device Date**, which allow you to set the 7X00 Control Module's internal clock; see **Setting the Device Date and Time**, [page 2-31](#)
- **System Group...**, which allows you to manage the SmartSwitch 7000 via SNMP MIB II. Refer to the *Generic SNMP User's Guide* for further information.

- **I/F Summary**, which lets you view statistics (displayed both graphically and numerically) for the traffic processed by each network interface on your device, and provides access to some SNMP MIB-II windows. See **Viewing I/F Summary Information**, [page 2-15](#), for details.
- **ATM Connections**, which launches the window that allows you to view and configure Permanent Virtual Circuits (PVCs) for any installed ATM interfaces. Note that this menu option will only appear when an ATM NIM module is installed in the chassis. For more information about configuring PVCs, see Chapter 6, **ATM Configuration**.
- **Com Port Configuration**, which allows you to configure the settings of the two COM ports on the 7X00 Control Module; see **Configuring the COM Ports**, [page 2-23](#), for details.
- **FDDI Statistics**, which lets you view a summary of traffic statistics for each installed FDDI interface. For more information, see **Viewing FDDI Statistics**, [page 2-20](#); note that this menu option will only appear when an FDDI NIM is installed in the chassis.
- **Bridge Status...**, which opens a window that provides an overview of bridging information for each port, and allows you to access all other bridge-related options. Refer to the bridging chapter of your *Tools Guide* for more information.
- **Find Source Address...**, which opens a window that allow you to search the SmartSwitch 7000's 802.1d Filtering Database to determine which bridging interface a specific MAC address is communicating through. If the MAC address is found, the port display will flash to indicate the correct bridge interface.
- **Exit**, which closes the SmartSwitch 7000 Chassis View window.

The Port Status Menu

The Port Status menu allows you to select the status information that will be displayed in the port text boxes in the Chassis View window:

- **Status** allows you to select one of four status type displays: Bridge, Bridge Mapping, Admin, or Operator.
- **Load** will display the portion of network load processed per polling interval by each interface, expressed as a percentage of the theoretical maximum load (10 or 100 Mbits/sec).
- **Errors** allows you to display the number of errors detected per polling interval by each interface, expressed as a percentage of the total number of valid packets processed by the interface.
- **I/F Mapping** will display the interface (if) index associated with each port your SmartSwitch 7000 chassis.
- **I/F Speed** will display the port's bandwidth: 10M (megabits) for Ethernet; 100M for Fast Ethernet, FDDI, or ATM.

- **I/F Type** will display the port type of each port in the SmartSwitch chassis: Eth (ethernet-csmacd) or FDDI.

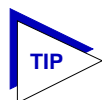
For more information on the port display options available via this menu, see **Selecting a Port Status View**, [page 2-10](#).

The FDDI Menu

If your SmartSwitch 7000 has one or more 7F06-02 modules installed, the FDDI menu will appear on the Chassis View menu bar, with the following options available for each SMT entity in the hub:

- **Configuration**
- **Connection Policy**
- **Station List**
- **Performance**

Refer to Chapter 5, **FDDI Management**, for more information on these selections.



*You can also view a summary of traffic statistics for each FDDI interface via the **FDDI Statistics** option available on the Device menu; see **Viewing FDDI Statistics**, [page 2-20](#), for more information.*

The Utilities Menu

The Utilities menu provides access to the MIB Tools utility, which provides direct access to the SmartSwitch 7000's MIB information, and to the RMON utility, a remote monitoring feature that is supported on a per-port basis when at least one Ethernet or Fast Ethernet NIM is installed in the chassis. These selections are also available from the **Utilities** menu at the top of the SPECTRUM Element Manager console window. Refer to your *Tools Guide* for a thorough explanation of the MIB Tools and RMON utilities.

The Help Menu

The Help Menu has three selections:

- **MIBs Supported**, which brings up the Chassis Manager window, described later in this chapter.
- **Chassis Manager Help**, which brings up a help window with information specifically related to using the Chassis Manager and Chassis View windows.
- **About Chassis Manager...**, which brings up a version window for the Chassis Manager application in use.

The Board Menus

The Board menu for the 7X00 Control Module (always installed in slot 1) provides mostly bridging-related selections, many of which are also available from the Bridge Status window:

- **Spanning Tree...**, which allows you to set bridge parameters when it is operating using the Spanning Tree Algorithm (STA) – the method that bridges use to decide the controlling (root) bridge when two or more bridges are in parallel. See the bridging chapter of your *Tools Guide* for more information.
- **Disable/Enable Bridge**, which enables or disables bridging across every interface installed in the SmartSwitch 7000 chassis.
- **Module Type...**, which brings up a window containing a description of the selected board; see **Viewing Hardware Types**, [page 2-13](#).
- **Performance Graph...**, which visually displays the combined performance of all bridging interfaces installed in the SmartSwitch 7000 hub; see the bridging chapter of your *Tools Guide*.

Board menus for other NIMs displayed in the Chassis View window provide only the **Module Type** selection.

The Port Menus

Each port menu offers the following selections:

- **Performance Graph...**, which brings up windows that visually display bridging performance at the selected interface; see the bridging chapter of your *Tools Guide* for details.
- **Source Addressing...**, which allows you to view the MAC addresses that are communicating through a selected bridge interface; see the bridging chapter of your *Tools Guide* for details.
- **I/F Statistics...**, which graphically displays color-coded statistical information for each bridge interface; see the bridging chapter of the *Tools Guide* for details.
- **Configuration...**, which launches the configuration window appropriate to the selected port: for standard Ethernet and FDDI ports, the configuration window allows you to set the Duplex Mode; for Fast Ethernet ports, it allows you to configure a number of different options, including auto-negotiation. See **Configuring Ports**, [page 2-23](#); note that there is no Configuration currently available for ATM ports.
- **Alarm Configuration...**, which launches the RMON-based Basic and Advanced Alarm applications; see Chapter 4, **Alarm Configuration**, for details. Note that this selection is available for all bridge port interfaces — even those (like FDDI and ATM) that do not specifically support RMON functionality — as long as at least one Ethernet or Fast Ethernet NIM is installed in the chassis.

- **Statistics...**, which launches the highest level of statistics currently available for the selected port. For standard Ethernet and Fast Ethernet ports, RMON statistics will be displayed if the RMON Default MIB component is active; if it has been disabled, MIB-II interface statistics will display. FDDI and ATM ports — which do not yet have their own RMON statistics groups — will always display MIB-II interface stats. See Chapter 3, **Statistics**, for more information.
- **Enable/Disable Port**, which disables bridging for the selected port; see Chapter 7, **Bridging**, and **Enabling and Disabling Ports**, [page 2-32](#), for more information.

Port Status Displays

When you open the Chassis View window, each port will display its current bridging state (defined below); to change this status display, select one of the options on the Port Status menu, as described in the following sections.

Selecting a Port Status View

To change the status view of your ports:

1. Click on **Port Status** on the menu bar at the top of the Chassis View window; a menu will appear.
2. Drag down (and to the right, if necessary) to select the status information you want to display. The port text boxes will display the appropriate status information.

Port status view options are:

Status

You can view four port status categories, as follows:

- **Bridge** — FWD, DIS, LRN, LIS, BLK, or BRK
- **Bridge Mapping** — bridge interface index numbers
- **Admin** — ON or OFF
- **Operator** — ON or OFF

If you have selected the **Bridge** status mode, a port is considered:

- **FWD** (Forwarding) if the port is on-line and ready to forward packets across the SmartSwitch 7000 from one network segment to another. Note that this is also the default display for ports which are administratively enabled but not connected.
- **DIS** (Disabled) if bridging at the port has been disabled by management; no traffic can be received or forwarded on this port, including configuration information for the bridged topology.

- LIS (Listening) if the port is not adding information to the filtering database. It is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move to the forwarding state.
- LRN (Learning) if the Forwarding database is being created, or the Spanning Tree Algorithm is being executed because of a network topology change. The port is monitoring network traffic, and learning network addresses.
- BLK (Blocking) if the port is on-line, but filtering traffic from going across the SmartSwitch 7000 from one network segment to another. Bridge topology information will be forwarded by the port.
- BRK (Broken) if the physical interface has malfunctioned.

If you have selected **Bridge Mapping**, the port status boxes will display the *bridge* interface index numbers assigned to each interface (which may or may not match the *ifIndex* values displayed via the **I/F Mapping** option described below).

If you have selected the **Admin** status mode, a port is considered:

- ON if the port is enabled by management.
- OFF if it has not been enabled or if it has been disabled through management action.

Note that the Admin state reflects the state *requested* by management; depending on the circumstances, this may or may not match the current Operator status, described below.

If you have selected the **Operator** status mode, a port is considered:

- ON if the port is currently forwarding packets.
- OFF if the port is not currently forwarding packets.

Note that the Operator status provides the *actual* status of the port; depending on the circumstances, this may or may not reflect the Admin state currently *requested* by management. For example, ports which are administratively ON but not yet connected would display an Operator status of OFF, since no packets are being forwarded.

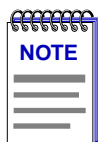
Load

If you choose **Load**, the interface text boxes will display the percentage of network load processed by each port during the last polling interval. This percentage reflects the network load generated per polling interval by devices connected to the port compared to the theoretical maximum load (10 or 100 Mbits/sec) of the connected network.

Errors

If you choose the **Errors** mode, the interface boxes will display the percentage of the total number of valid packets processed by each port during the last polling interval that were error packets. This percentage reflects the number of errors

generated during the last polling interval by devices connected to that port compared to the total number of valid packets processed by the port.



*In SPECTRUM Element Manager, the polling interval is set via the **Tools—>Options** selection from the primary window menu.*

*Refer to the **SPECTRUM Element Manager User's Guide** for full information on setting device polling intervals.*

I/F Mapping

If you choose the I/F Mapping mode, the interface boxes will display the interface number (IfIndex) associated with each port in the SmartSwitch 7000 chassis.

I/F Speed

If you choose the I/F Speed mode, the interface boxes will display the bandwidth of each individual port in the SmartSwitch 7000 chassis: 10M (megabits) for standard Ethernet; 100M for Fast Ethernet, FDDI, and ATM.

I/F Type

If you choose the I/F Type mode, the interface boxes will display the network type supported by each interface installed in the SmartSwitch 7000 chassis: Eth (ethernet-csmacd), FDDI, or ATM. Note that there is no type distinction between standard Ethernet and Fast Ethernet.

Port Status Color Codes

Three of the Port Status display options — Bridge, Admin, and Operator — incorporate their own color coding schemes: for the Bridge option, green = FWD, blue = DIS, magenta = LIS or LRN, orange = BLK, and red = BRK; for Admin and Operator, green = ON, red = OFF, and blue = N/A (not available).

For all other Port Status selections — Load, Errors, I/F Mapping, I/F Speed, and I/F Type — color codes will continue to reflect the most recently selected mode which incorporates its own color coding scheme.

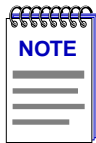
The Chassis Manager Window

Like most networking devices, Cabletron's devices draw their functionality from a collection of proprietary MIBs and IETF RFCs. In addition, Cabletron's newer intelligent devices — like the SmartSwitch 7000 — organize their MIB data into a series of "components." A MIB component is a logical grouping of MIB data, and each group controls a defined set of objects. For example, SmartSwitch 7000 bridging information is organized into its own component; RMON, Distributed LAN Monitor (DLM), and FDDI SMT information are also contained in separate components. Note, too, that there is no one-to-one correspondence between MIBs and MIB components; a single MIB component might contain objects from several different proprietary MIBs and RFCs.

The Chassis Manager window, [Figure 2-4](#), is a read-only window that displays the MIBs and the MIB components — and, therefore, the functionality — supported by the currently monitored device.

To view the Chassis Manager window:

1. Click on **Help** on the far right of the menu bar at the top of the chassis manager window.
2. Drag down to **MIBs Supported**, and release.



The Chassis Manager window will also appear briefly when the Chassis View window is launched.

MIB Components are listed here; remember, there's no one-to-one correspondence between MIBs and MIB Components

The MIBs which provide the SmartSwitch 7000's functionality — both proprietary MIBs and IETF RFCs — are listed here

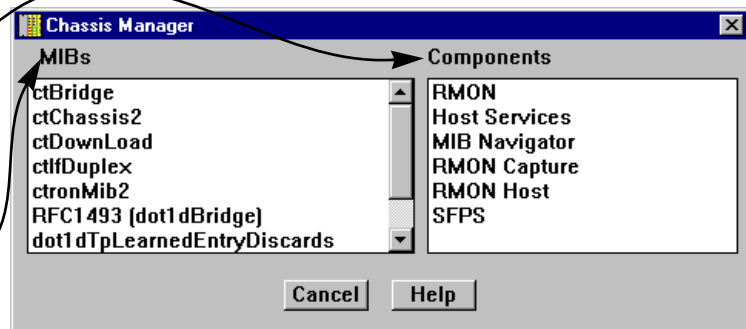


Figure 2-4. Chassis Manager Window

Viewing Hardware Types

In addition to the graphical displays described above, menu options available at the device and board levels provide specific information about the physical characteristics of the SmartSwitch 7000 hub and its installed modules.

Device Type

Choosing the **Device Type** option on the Device menu brings up a window that describes the management device being modeled:

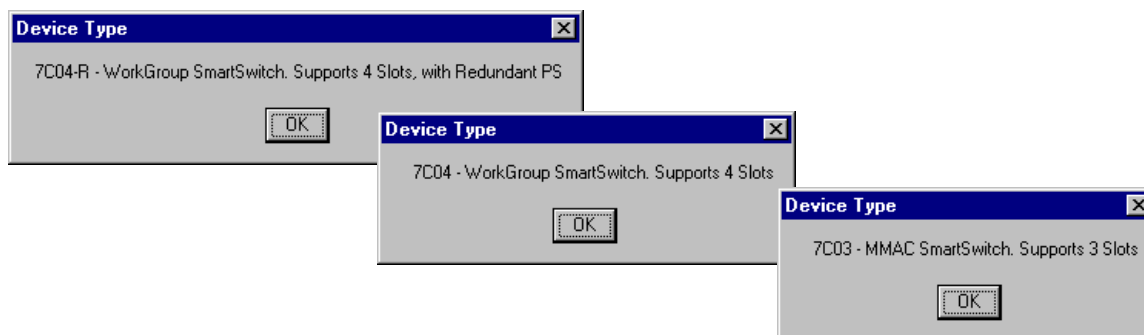


Figure 2-5. Device Type Windows

Module Type

From the Board menus on the SmartSwitch 7000 Chassis View window, you can view a description of the Module types installed in your SmartSwitch chassis.

To view a Module type:

1. Click on the desired **Board** number. The Board menu will appear.
2. Drag down to **Module Type....** A Module Type text box (similar to the examples shown in [Figure 2-6](#)) will appear, describing the board type.

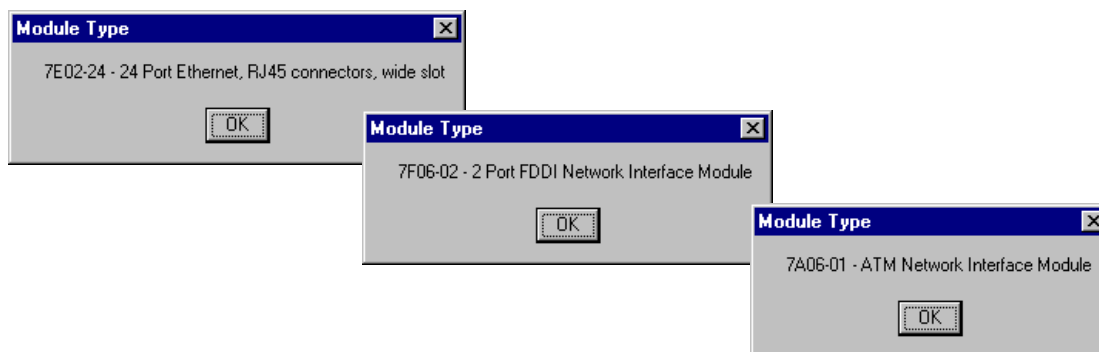


Figure 2-6. Sample Module Type Text Boxes

Viewing I/F Summary Information

The **I/F Summary** menu option available from the Device menu lets you view statistics for the traffic processed by each network interface on your device. The window also provides access to a detailed statistics window that breaks down Transmit and Receive traffic for each interface.

To access the I/F Summary window:

1. From the Module View, click on the **Device** option from the menu bar.
2. Click again to select **I/F Summary**, and release. The I/F Summary window, [Figure 2-7](#), will appear.

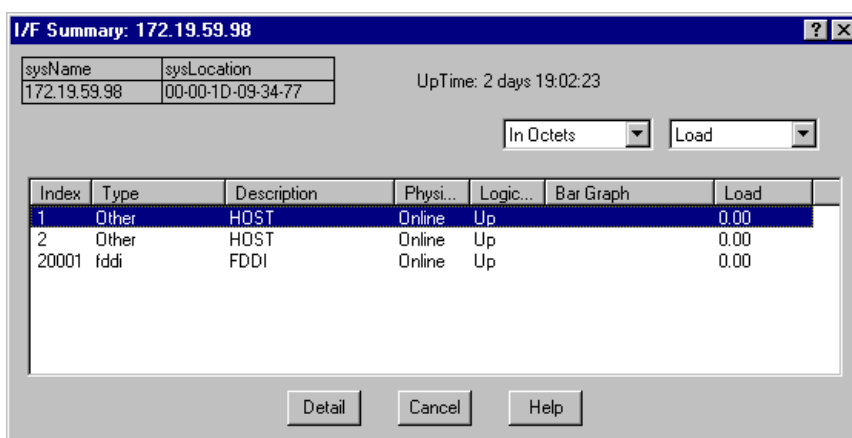


Figure 2-7. I/F Summary Window

The I/F Summary window provides a variety of descriptive information about each interface on your device, as well as statistics which display each interface's performance.

The following descriptive information is provided for each interface:

UpTime

The **UpTime** field lists the amount of time, in a days, hh:mm:ss format, that the device has been running since the last start-up.

Index

The index value assigned to each interface on the device.

Type

The type of the interface, distinguished by the physical/link protocol(s) running immediately below the network layer. Possible values are **Other** (for the 7X00 Controller Module's two backplane Host interface), **fdi**, and **ethernet-csmacd** (for both standard and Fast Ethernet interfaces), and **atm**.

Description

A text description of the interface: **Host** (for the 7X00 Controller Module's two backplane interfaces); **FDDI**, **Ethernet** (for both standard and Fast Ethernet front panel interfaces), and **ATM**.

Physical Status

Displays the current physical status — or operational state — of the interface: **Online** or **Offline**.

Logical Status

Displays the current logical status — or administrative state — of the interface: **Up** or **Down**.

Interface Performance Statistics/Bar Graphs

The statistical values (and, where available, the accompanying bar graphs) to the right of the interface description fields provide a quick summary of interface performance. You can select the statistical value you want to display and the units in which you want those values displayed by using the two menu fields directly above the interface display area, as follows:

1. In the right-most menu field, click on the down arrow and select the unit in which you wish to display the selected statistic: **Load**, **Raw Counts**, or **Rate**.



*Bar graphs are only available when **Load** is the selected base unit; if you select **Raw Counts** or **Rate**, the Bar Graph column will be removed from the interface display.*

2. Once you have selected the base unit, click on the down arrow in the left-most field to specify the statistic you'd like to display. Note that the options available from this menu will vary depending on the base unit you have selected.

After you select a new display mode, the statistics (and graphs, where applicable) will refresh to reflect the current choice, as described below.

Raw Counts

The total count of network traffic received or transmitted on the indicated interface since device counters were last reset. Raw counts are provided for the following parameters:

In Octets	Octets received on the interface, including framing characters.
In Packets	Packets (both unicast and non-unicast) received by the device interface and delivered to a higher-layer protocol.

In Discards	Packets received by the device interface that were discarded even though no errors prevented them from being delivered to a higher layer protocol (e.g., to free up buffer space in the device).
In Errors	Packets received by the device interface that contained errors that prevented them from being delivered to a higher-layer protocol.
In Unknown	Packets received by the device interface that were discarded because of an unknown or unsupported protocol.
Out Octets	Octets transmitted by the interface, including framing characters.
Out Packets	Packets transmitted, at the request of a higher level protocol, by the device interface to a subnetwork address (both unicast and non-unicast).
Out Discards	Outbound packets that were discarded by the device interface even though no errors were detected that would prevent them from being transmitted. A possible reason for discard would be to free up buffer space in the device.
Out Errors	Outbound packets that could not be transmitted by the device interface because they contained errors.

Load

The number of bytes processed by the indicated interface during the last poll interval in comparison to the theoretical maximum load for that interface type (10 Mbps for standard Ethernet; 100 Mbps for Fast Ethernet, FDDI, or ATM). Load is further defined by the following parameters:

In Octets	The number of bytes received by this interface, expressed as a percentage of the theoretical maximum load.
Out Octets	The number of bytes transmitted by this interface, expressed as a percentage of the theoretical maximum load.

When you select this option, a Bar Graph field will be added to the interface display area; this field is only available when **Load** is the selected base unit.

Rate

The count for the selected statistic during the last poll interval. The available parameters are the same as those provided for Raw Counts. Refer to the Raw Counts section, above, for a complete description of each parameter.

Viewing Interface Detail

The Interface Statistics window (Figure 2-8) provides detailed MIB-II interface statistical information — including counts for both transmit and receive packets, and error and buffering information — for each individual port interface. Color-coded pie charts also let you graphically view statistics for both received and transmitted Unicast, Multicast, Discarded, and Error packets.

To open the Interface Statistics window:

1. In the I/F Summary window, click to select the interface for which you'd like to view more detailed statistics.
2. Click on **Detail**. The appropriate I/F Statistics window, Figure 2-8, will appear.

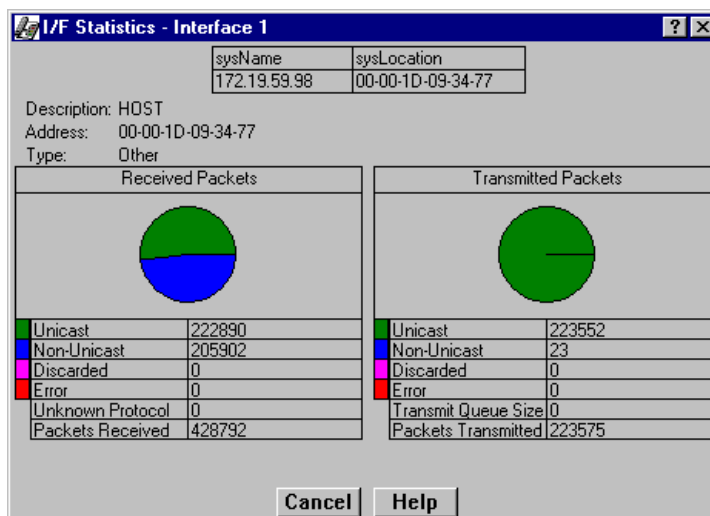
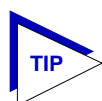


Figure 2-8. Detail Interface Statistics



You can also access this information via the I/F Statistics option available on the individual port menus; see Chapter 3, **Statistics**, for more information.

Three informational fields appear in the upper portion of the window:

Description

Displays the interface description for the currently selected interface: Ethernet, FDDI, ATM, or Host.

Address

Displays the MAC (physical) address of the selected interface.

Type

Displays the interface type of the selected port: ethernet-csmacd, fddi, atm, or other.

The lower portion of the window provides the following transmit and receive statistics; note that the first four statistics are also graphically displayed in the pie charts.

Unicast

Displays the number of packets transmitted to or received from this interface that had a single, unique destination address. These statistics are displayed in the pie chart, color-coded green.

Non-Unicast

Displays the number of packets transmitted to or received from this interface that had a destination address that is recognized by more than one device on the network segment. The multicast field includes a count of broadcast packets — those that are recognized by *all* devices on a segment. These statistics are displayed in the pie chart, color-coded dark blue.

Discarded

Displays the number of packets which were discarded even though they contained no errors that would prevent transmission. Good packets are typically discarded to free up buffer space when the network becomes very busy; if this is occurring routinely, it usually means that network traffic is overwhelming the device. To solve this problem, you may need to re-configure your bridging parameters, or perhaps re-configure your network to add additional bridges or switches. Consult the Cabletron Systems *Network Troubleshooting Guide* for more information.

These statistics are displayed in the pie chart, color-coded magenta.

Error

Displays the number of packets received or transmitted that contained errors. These statistics are displayed in the pie chart, color-coded red.

Unknown Protocol (Received only)

Displays the number of packets received which were discarded because they were created under an unknown or unsupported protocol.

Packets Received (Received only)

Displays the number of packets received by the selected interface.

Transmit Queue Size (Transmit only)

Displays the number of packets currently queued for transmission from this interface. The amount of device memory devoted to buffer space, and the traffic level on the target network, determine how large the output packet queue can grow before the SmartSwitch 7000 module will begin to discard packets.

Packets Transmitted (*Transmit only*)

Displays the number of packets transmitted by this interface.

Making Sense of Detail Statistics

The statistics available in this window can give you an idea of how an interface is performing; by using the statistics in a few simple calculations, it's also possible to get a sense of an interface's activity level:

To calculate the percentage of input errors:

Received Errors /Packets Received

To calculate the percentage of output errors:

Transmitted Errors /Packets Transmitted

To calculate the total number of inbound and outbound discards:

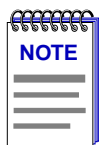
Received Discards + Transmitted Discards

To calculate the percentage of inbound packets that were discarded:

Received Discards /Packets Received

To calculate the percentage of outbound packets that were discarded:

Transmit Discards /Packets Transmitted



Unlike the Interface Detail window, which this window replaces, the Interface Statistics window does not offer **Disable** or **Test** options. These options are available in the Interface Group window, which can be accessed via the System Group window (select **System Group...** from the **Device** menu). Refer to your **Generic SNMP User's Guide** for further information on the System Group and Interface Group windows.

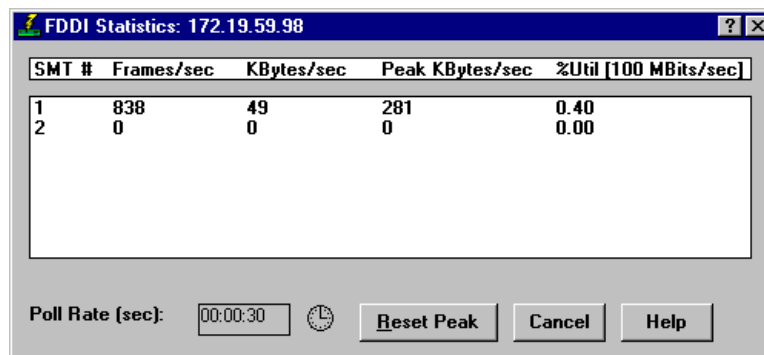
Viewing FDDI Statistics

The FDDI Statistics window, [Figure 2-9](#), provides basic information concerning the ring networks supported by the SmartSwitch 7000's SMT entities — including bandwidth utilization expressed in terms of frames/second (current) and kilobytes/second (both current and peak experienced since last reset), and current utilization as a percentage of theoretical maximum.

A timer interval lets you set the interval at which you want the SmartSwitch 7000's installed FDDI NIMs polled for this information.

To access the FDDI Statistics window:

1. In the Chassis View, click on **Device**.
2. Drag down to **FDDI Statistics...** and release. The FDDI Statistics window will appear.



SMT #	Frames/sec	KBytes/sec	Peak KBytes/sec	%Util [100 Mbits/sec]
1	838	49	281	0.40
2	0	0	0	0.00


Poll Rate (sec): 00:00:30  **Reset Peak** **Cancel** **Help**

Figure 2-9. The FDDI Statistics Window

The FDDI Statistics window contains the following fields:

SMT #

The index number of the SMT entity to which the statistics entries pertain.

Frames/sec

The current bandwidth, expressed in terms of frames per second.

KBytes/sec

The current bandwidth, expressed in terms of kilobytes per second.

Peak KBytes/sec

The most kilobytes per second experienced on the ring associated with the SMT entity since peak FDDI statistics counters were last reset for the device.


You can reset the peak value at any time by clicking **Reset Peak**.

%Util (100 Mbits/sec)

The current percentage of bandwidth utilized on the network in comparison to its theoretical maximum bandwidth (100 Mbps for an FDDI network). This is calculated by using the following formula: $(\text{current Kbps} \times 8) / 1000$.

Setting the FDDI Statistics Polling Interval

To set the interval at which you want the SmartSwitch 7000 polled for FDDI Statistics:

1. Click on  next to the **Peak Rate (sec):** field. The New Timer Interval window, [Figure 2-10](#), will appear.

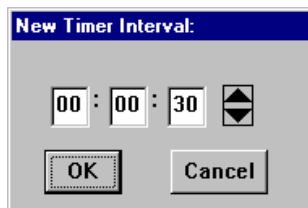


Figure 2-10. New Timer Interval Window

2. Highlight the **Hour**, **Minute**, or **Second** field, and type in a new value. The allowable range is from 1 second to 23:59:59.

You can also highlight each field, and use the Up and Down scroll arrows to increase or decrease the value.

3. Click on **OK** to accept the new interval, or on **Cancel** to exit without making any changes.

Using the Find Source Address Feature

You can use the Find Source Address option to discover the bridging interface through which a specific MAC address is communicating with the SmartSwitch 7000. When you select **Find Source Address** from the Device menu, the device's Filtering Database is searched for an entry which designates the bridge interface serving as the source port for packets from the selected MAC address. If the search is successful, the associated port will flash on the Chassis View display; if the search is unsuccessful, a window will appear indicating that fact.

To search for a source address:

1. Click on **Device** in the Chassis View window to display the Device menu.
2. Drag down to **Find Source Address...**, and release. The Find Source Address window, [Figure 2-11](#), will appear.

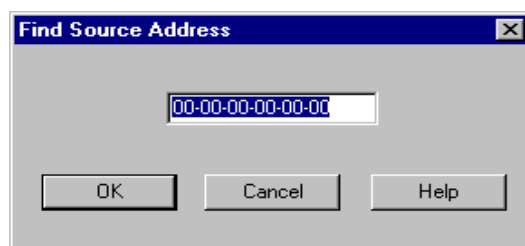


Figure 2-11. Find Source Address Window

3. In the text field, enter a valid MAC address in hexadecimal format, then click **OK**. If you enter an invalid address — that is, one not in hexadecimal xx-xx-xx-xx-xx-xx- format — an error window will appear indicating that the selected address is invalid.

If the selected MAC address is found in the SmartSwitch 7000's Filtering Database, the bridge interface through which the address is communicating will flash in the Chassis View display.

If the address is not found, a window will appear indicating that the address could not be found.

Managing the Hub

In addition to the performance and configuration information described in the preceding sections, the Chassis View also provides you with the tools you need to configure your SmartSwitch hub and keep it operating properly. Hub management functions include setting operating parameters for Ethernet, FDDI, Fast Ethernet, and COM ports; setting device date and time; and enabling and disabling bridging at specific port interfaces.

Configuring Ports

The Configuration options available for FDDI, Ethernet, Fast Ethernet, and COM ports allow you to configure operating parameters specific to each port type: for FDDI and standard Ethernet ports, you can set the Duplex Mode; for Fast Ethernet ports, you can set a variety of duplex mode and negotiation parameters; and for COM ports, you can select the operation you wish the port to perform, and set any associated speed parameters. FDDI, Ethernet, and Fast Ethernet Port Configuration windows are available from the Chassis View Port menus; the COM Port option is available from the Device menu. Note that no configuration option currently exists for ATM ports.

Configuring Ethernet and FDDI Ports

The Port Configuration window available for both standard Ethernet and FDDI ports allows you to set an interface to either Standard or Full Duplex Mode. Full Duplex mode effectively doubles the available wire speed by allowing the interface to both receive and transmit simultaneously. This window will also display the mode currently in effect on the selected interface.

To access the Port Configuration Window:

1. From the Chassis View, click to select the port you wish to configure; the Port Menu will display.
2. Drag down to **Configuration**, and release. The Port Configuration window, [Figure 2-12](#), will appear.

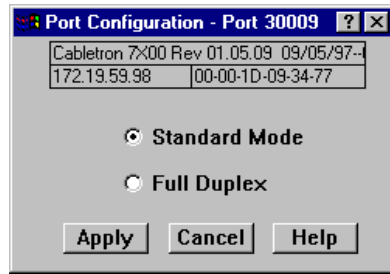
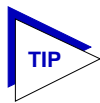


Figure 2-12. Port Configuration



*Note that, if you select the Configuration option available for a Fast Ethernet interface, an entirely different window will appear; see **Configuring Fast Ethernet Ports**, below, for information on configuring these ports.*

Use the options in this window to select the desired mode:

Standard Mode

In Standard Mode, an interface can only either transmit *or* receive at any given time, and must wait for one activity to be completed before switching to the next activity (receive or transmit). In this mode, standard wire speeds (10 Mbps for Ethernet, 100 Mbps for FDDI) are available.

Full Duplex

In Full Duplex Mode, an interface can both receive *and* transmit packets at the same time, effectively doubling the available wire speed to 20 Mbps (for Ethernet) or 200 Mbps (for FDDI).

Be sure to click on **Apply** to set your changes; note that the interface's current mode can be determined by the field selected in the window.

Configuring Fast Ethernet Ports

If you have any Fast Ethernet NIMs installed in your SmartSwitch 7000 chassis, the Port Configuration window available for those ports allows you to both view and set that port's available modes. All 100Base-TX Fast Ethernet ports can be configured to operate in either standard Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) mode, and in each mode can be configured to operate in Full Duplex, effectively doubling the available wire speed (from 10 to 20 Mbps in standard Ethernet mode, or from 100 to 200 Mbps in Fast Ethernet mode); 100Base-FX (fiber) ports can be configured to operate in their standard 100 Mbps mode, or in full duplex mode. This window also displays the mode currently in effect on the selected interface, and provides some information (where it is available) about the interface's link partner.

To access the Port Configuration Window:

1. From the Chassis View, click to select the port you wish to configure; the Port Menu will display.
2. Drag down to **Configuration**, and release. The Fast Ethernet Port Configuration window, [Figure 2-13](#), will appear.

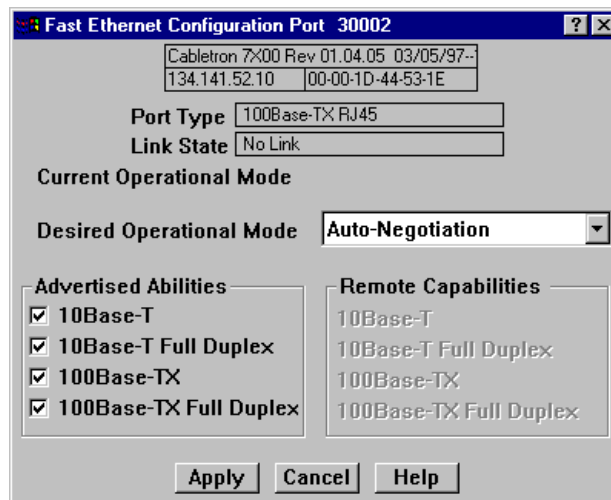
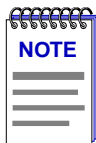
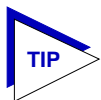


Figure 2-13. Fast Ethernet Configuration



The Advertised Abilities functionality is not supported by the FE-100FX Fast Ethernet port module; if you launch the Configuration window for one of these modules, the **Advertised Abilities** and **Remote Capabilities** sections of the window will be grayed out. If you launch the window for a port module slot which has no FE module installed, the Port Type will display as Unknown, the Link State will display No Link, and the rest of the fields will be blank and/or grayed out.



Note that, if you select the Configuration option available for a standard Ethernet or FDDI interface, an entirely different window will appear; see **Configuring Ethernet and FDDI Ports**, [page 2-23](#), for information on configuring these ports.

From this window you can manually set the operational mode of the port, or — for 100Base-TX interfaces — set the port to auto negotiation so that the appropriate operational mode can be determined automatically. The mode you set will determine the speed of the port and whether it uses Full Duplex or Standard Mode bridging.

The following information about the selected Fast Ethernet port is displayed:

Port Type

Displays the port's type: 100Base-TX RJ-45 (for built-in Fast Ethernet ports and the FE-100TX Fast Ethernet port module), 100Base-FX MMF SC Connector (for the FE-100-FX Fast Ethernet port module), or Unknown (for a port slot with no module installed).

Link State

Displays the current connection status of the selected port: Link or No Link.

Current Operational Mode

Indicates which of the available operational modes is currently in effect: 10Base-T, 10Base-T Full Duplex, 100Base-TX, 100Base-TX Full Duplex, 100Base-FX, or 100Base-FX Full Duplex. If the port is still initializing, not linked, or if there is no port module installed in the slot, this field will remain blank.

Desired Operational Mode

Displays the operational mode that you have selected for this port, and allows you to change that selection. The following operational modes are available for each port:

100Base-TX Auto Negotiation, 10Base-T, 10BASE-T Full Duplex, 100Base-TX, and 100Base-TX Full Duplex.

100Base-FX 100Base-FX and 100Base-FX Full Duplex



If you choose to select a specific mode of operation (rather than auto-negotiation), you should be sure that the link partner supports the same mode. Otherwise, no link will be achieved.

If you select a Full Duplex mode and the link partner supports the same wire speed but not Full Duplex, a link will be achieved, but it will be unstable and will behave erratically.

If you select Auto-Negotiation, the local node will try to match the mode of the link partner, even if the link partner is not set to auto-negotiate, and even if the local node must use a mode which is it is not currently advertising.

Note that if Auto Negotiation is the selected mode, the **Current Operational Mode** field will indicate which mode was selected by the link partners.

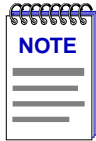
See **Setting the Desired Operational Mode**, [page 2-27](#), for more information.

Advertised Abilities

For 100Base-TX ports which have been configured to operate in Auto Negotiation mode, this field allows you to select which of the operational modes available to the port can be selected by the negotiating link partners. During Auto Negotiation, each of the link partners will advertise all selected modes in descending bandwidth order: 100Base-TX Full Duplex, 100Base-TX, 10Base-T Full

Duplex, and 10Base-T. Of the selected abilities, the highest mode mutually available will automatically be used. If there is no mode mutually advertised, no link will be achieved.

If you have selected a specific operational mode for your 100Base-TX port, the Advertised Abilities do not apply; the selected Advertised Abilities also do not restrict the local node's ability to set up a link with a partner who is not currently Auto-Negotiating.



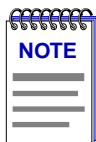
Auto-Negotiation is not currently supported for 100Base-FX ports; for these ports, the Advertised Abilities section will be grayed out.

Remote Capabilities

When the local node is set to Auto-Negotiation, this field will display the advertised abilities of the remote link — even if the remote link is not currently set to auto-negotiate. Possible values for this field are:

- 100Base-TX Full Duplex
- 100Base-TX
- 10Base-T Full Duplex
- 10Base-T
- Link Partner does not support auto negotiation — auto negotiation is either not supported by or is not currently selected on the remote port.
- Unknown — the link partner's capabilities could not be determined.

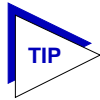
When the local node is *not* set to Auto-Negotiation, this field will be grayed out, even if the link partner is set to Auto-Negotiation and is advertising abilities.



If both link partners are set to Auto-Negotiation, but there is no mutually-advertised operational mode, no link will be achieved, and both nodes may display the message "Link Partner does not support Auto-Negotiation." To resolve this situation, be sure both link partners advertise all their abilities, or be sure they advertise at least one mutually-available mode.

Setting the Desired Operational Mode

For any 100Base-TX port, you can specifically choose any one of the four available operational modes, or you can select Auto-Negotiation mode, which allows the port to negotiate with its link partner to find the highest mutually available bandwidth. If you select Auto Negotiation mode, you must also choose which of the port's bandwidth capabilities you wish to advertise to the link partner.



If you select Auto-Negotiation at both ends of a link, be sure at least one mutually-advertised operational mode is available.

For a 100Base-FX port, the selection process is somewhat simpler; Auto Negotiation for these ports is not supported at this time, so you need only choose between 100Base-FX standard mode and 100Base-FX Full Duplex. However, you must still be sure that both link partners are set to the same operational mode, or the link will be unstable.

To set your desired operational mode:

1. Click in the **Desired Operational Mode** field to display the menu of available options; drag down to select the operational mode you wish to set.

For 100Base-TX ports, the available options are:

10Base-T — 10 Mbps connection, Standard Mode

10Base-T Full Duplex — 10 Mbps connection, Duplex Mode

100Base-TX — 100 Mbps connection, Standard Mode

100Base-TX Full Duplex — 100 Mbps connection, Duplex Mode

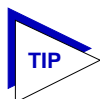
Auto Negotiation — the operational mode will be dynamically set based on the modes selected in the Advertised Abilities field (where both link partners are auto-negotiating) and the speeds and modes supported by the attached device

For 100Base-FX ports, options are:


100Base-FX — 100 Mbps connection, Standard Mode

100Base-FX Full Duplex — 100 Mbps connection, Duplex Mode

2. If you have selected Auto Negotiation (for 100Base-TX ports only), use the **Advertised Abilities** field to select the operational capabilities you wish to advertise to the port's link partner. If both link partners will be auto-negotiating, be sure there is at least one mutually-advertised operational mode, or no link will be achieved.



The selected Advertised Abilities only come into play when both link partners are auto-negotiating; if only one link partner is set to auto-negotiate, that node will establish a link at whatever mode its partner is set to, even if that mode is not currently being advertised.

3. Click on  to save your changes. Some window fields will refresh immediately and display the new settings; to manually refresh the window, simply close, the re-open it, or just re-select the **Configuration** option from the appropriate Port menu. Note that it may take a few minutes for mode

changes to be completely initialized, particularly if the link partners must negotiate or re-negotiate the mode; you may need to refresh the window a few times before current operational data is displayed.

Configuring the COM Ports

You can use the COM Port Configuration window (Figure 2-14) to specify the functions each of the RS232 COM ports on the 7X00 Control Module face will perform. To do so:

1. Click on **Device** in the Chassis View menu bar to display the Device menu.
2. Drag down to **COM Port Configuration**, then right to select **Port 1** or **Port 2**, and release. The COM Port Configuration window, Figure 2-14, will appear.

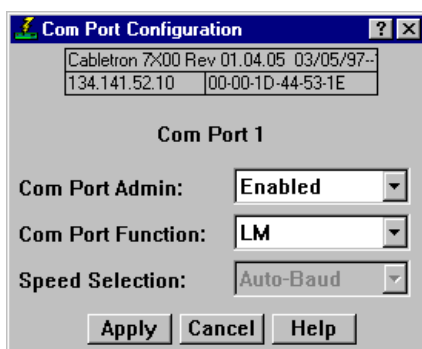


Figure 2-14. COM Port Configuration

You can use the COM Port Configuration window to set the following operating parameters:

COM Port Admin

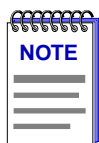
Use this field to administratively enable or disable the selected COM port.

COM Port Function

Use this field to select the function for which you wish to use the selected COM port:

LM	Local Management: select this option if you wish to connect a terminal to the selected COM port from which to run Local Management.
UPS	Select this option if you wish to connect an uninterruptable power supply (UPS) to the selected COM Port. Note that if you select this option, an additional option — UPS — will appear on the Device menu; use the resulting window to configure specific UPS settings.

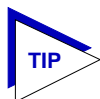
- | | |
|------|--|
| SLIP | Select this option to use the selected COM port as a SLIP connection for out-of-band SNMP management via direct connection to a serial port on your network management workstation. Note that when you configure the port as a SLIP connection, you must select the desired baud rate in the Speed Selection field described below. |
| PPP | Select this option to use the selected COM port as a PPP connection for out-of-band SNMP management via direct connection to a serial port on your network management workstation. Note that when you configure the port as a PPP connection, you must select the desired baud rate in the Speed Selection field described below. |



Current 7X00 firmware versions support only Local Management and UPS via the COM ports; future versions will add SLIP and PPP support.



Speed Selection

If you have configured the selected port as a SLIP or PPP connection, you must select the appropriate baud rate: 2400, 4800, 9600, or 19,200. Note that this field will default to Auto-Baud and become unselectable when the **COM Port Function** is set to LM or UPS.



*If the COM port you wish to configure is currently set to LM or UPS, the **Speed Selection** field will be unavailable until the COM Port Function is set to SLIP or PPP and that change is applied. Once available, the Speed Selection field will default to the last known speed setting; use the down arrow to change this setting if necessary, then click **Apply** again to complete the configuration.*

To change the configuration of the selected COM port:

1. Click on the  to the right of each field.
2. Drag down to select the desired setting, then release.
3. Click on  to save your changes.

Setting the Device Date and Time

The **Device** menu provides the options that allow you to change the date and time stored in the device's internal clock: **Edit Device Time** and **Edit Device Date**.

To edit the device time:

1. Click on **Device** on the Chassis View window menu bar to access the Device menu; drag down to **Edit Device Time**, and release.
2. The Device Time change window, [Figure 2-15](#), will appear.

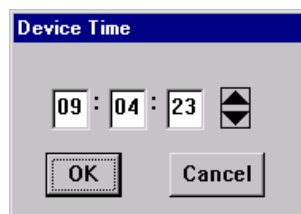


Figure 2-15. Edit Time Window

3. Enter the new time in a 24-hour hh:mm:ss format, either by highlighting the field you wish to change and using the up and down arrow buttons, or by simply entering the new value in the appropriate field.
4. Click on **OK** to save your changes, or on **Cancel** to cancel.

To edit the device date:

1. Click on **Device** on the Chassis View window menu bar to access the Device menu; drag down to **Edit Device Date**, and release.
2. The Device Date change window, [Figure 2-16](#), will appear.

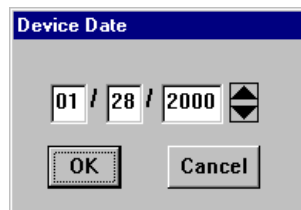


Figure 2-16. Edit Date Window

3. Enter the new date in a mm/dd/yyyy format, either by highlighting the field you wish to change and using the up and down arrow buttons, or by simply entering the new value in the appropriate field.
4. Click on **OK** to save your changes, or on **Cancel** to cancel.



In accordance with Year 2000 compliance requirements, SPECTRUM Element Manager now displays and allows you to set all dates with four-digit year values.

Enabling and Disabling Ports

When you disable bridging at a port interface, you disconnect that port's network from the bridge entirely. The port does not forward any packets, nor does it participate in Spanning Tree operations. Nodes connected to the network can still communicate with each other, but they can't communicate with the bridge or with other networks connected to the bridge. When you enable bridging for the interface, the port moves from the Disabled state through the Listening and Learning states to the Forwarding state; bridge port state color codes will change accordingly.

To enable or disable bridging for an individual interface:

1. Click on the appropriate port display box to display the port menu.
2. Drag down to select **Enable** to enable bridging at the interface, or **Disable** to disable bridging. Bridging will now be enabled or disabled across the selected port, as desired.

To enable or disable bridging for all interfaces installed in the SmartSwitch 7000 chassis:

1. Click on the module index for the 7X00 Control Module (always installed in slot 1) to display the 7X00 Module menu.
2. Drag down to select **Enable Bridge** to enable bridging at all installed interfaces, or **Disable Bridge** to disable bridging across all interfaces. Bridging will now be enabled or disabled across the installed interfaces, as desired.

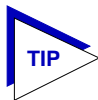


*For more information about bridging functions and how to determine the current state of each bridge port, see the bridging chapter of your **Tools Guide**.*

Statistics

Accessing interface statistics from the Chassis View; available statistics windows

Selecting the Statistics option from the port interface displays in the chassis view will launch the highest level of statistics available for the selected interface: if the interface supports RMON, the appropriate RMON Ethernet statistics will display; if RMON is not supported by the interface — or if the RMON Default MIB component is inactive — MIB-II interface (IF) statistics will display.



Since the SmartSwitch 7000 does provide RMON support, selecting the Statistics option for any Ethernet or Fast Ethernet interface will launch the appropriate RMON statistics (as long as the RMON MIB component is enabled). For FDDI and ATM interfaces — which do not specifically support RMON stats — the MIB-II interface statistics will display.

*Note, too, that the MIB-II IF Statistics window is also available for all port interfaces — regardless of their level of RMON support or the current administrative status of the RMON Default MIB component — via the I/F Summary window (described in **Chapter 2**) or the bridge port menus in the Bridge Status view (described in the **Bridging Chapter** in the **Tools Guide**).*

Accessing the Statistics Window

To access the available statistics for each interface:

1. In the Chassis View window, click on the appropriate port interface to display the Port menu.
2. Drag down to **Statistics**, and release. The RMON Statistics ([Figure 3-1, page 3-2](#)) or MIB-II IF Statistics window ([Figure 3-3, page 3-7](#)), as appropriate, will appear.



If the selected interface displays MIB-II IF Statistics and you were expecting to see RMON statistics, the RMON Default MIB component may be disabled; see the **RMON** chapter in the **Tools Guide** for information on how to check (and, if necessary, change) the administrative status of the RMON MIB component.

Note, too, that Token Ring statistics are not covered in this chapter, as there are currently no Token Ring NIMs available for the SmartSwitch 7000 hub.

RMON Statistics

The RMON Ethernet Statistics window (Figure 3-1) provides a detailed statistical breakdown of traffic on the selected Ethernet network. Statistics are provided in both numerical and graphic format, and include peak values and the date and time they occurred.

The selected interface number and its description are displayed at the top of the Statistics window, along with the four boxes indicating the device's name, location, IP address, and MAC address.

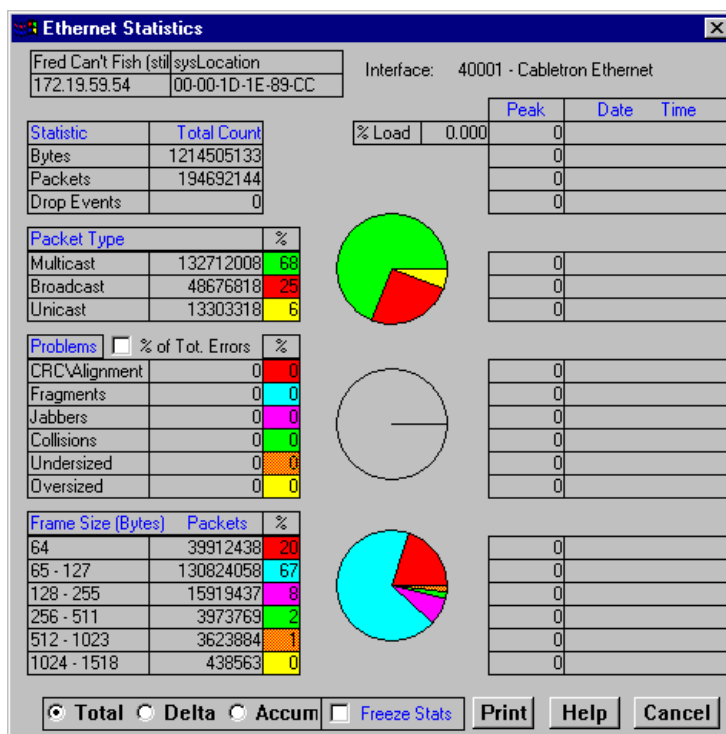


Figure 3-1. The Ethernet Statistics Window

The column on the left side of the window displays the statistic name, total count, and percentage; the column on the right displays the peak value for each statistic, and the date and time that value occurred. Note that peak values are always Delta values; see [Viewing Total, Delta, and Accumulated Statistics, page 3-5](#), for more information.

Ethernet statistics are:

Bytes

Displays the total number of bytes contained in packets processed on the network segment. This number includes bytes contained in error packets.

Packets

Displays the total number of packets processed on the network segment. Again, this number includes error packets.

Drop Events

This field indicates the number of times packets were dropped because the device could not keep up with the flow of traffic on the network. Note that this value does not reflect the number of packets dropped, but only the number of times packets were dropped.

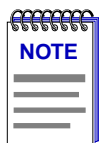
% Load

Displays the network segment load during the sample interval, in hundredths of a percent; this percentage reflects the network segment load compared to the theoretical maximum load (10 Mbits/sec) of an Ethernet network.

Packet Type

Multicast	Indicates the number of good packets processed on the network segment that were destined for more than one address. Note that this total does not include broadcast packets.
Broadcast	Indicates the number of good packets processed on the network segment that had the broadcast (FF-FF-FF-FF-FF-FF) destination address.
Unicast	Indicates the number of good packets processed on the network segment that were destined for a single address.

The percentages displayed to the right of the numerical values for these fields indicate what percentage of good packets transmitted on the network segment were multicast, broadcast, and unicast; these percentages will add up to 100. The pie chart in the center of the window provides a graphical view of the percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.

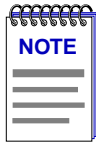


If you reset your device, you must first close, then re-open the Statistics window to refresh peak values.

Problems

CRC/Alignment	Indicates the number of packets processed by the network segment that had a non-integral number of bytes (alignment error) or a bad frame check sequence (Cyclic Redundancy Check, or CRC error).
Fragments	Indicates the number of packets processed by the network segment that were undersized (less than 64 bytes in length; a runt packet) <i>and</i> had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).
Jabbers	Indicates the number of packets processed by the network segment that were oversized (greater than 1518 bytes; a giant packet) <i>and</i> had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).
Collisions	Indicates the total number of receive (those the device detects while receiving a transmission) and transmit (those the device detects while transmitting) collisions detected on the network segment.
Undersized	Indicates the number of packets processed by the network segment that contained fewer than 64 bytes (runt packets) but were otherwise well-formed.
Oversized	Indicates the number of packets processed by the network segment that contained more than 1518 bytes (giant packets) but were otherwise well-formed.

In their default state, the percentages displayed to the right of the numerical values for these fields indicate what percentage of **total packets** transmitted on the network segment were of the noted type. If you select the **% of Tot. Errors** option by clicking the mouse button in the check box, the percentages will indicate what percentage of **problem, or error, packets** transmitted on the network segment were of the noted type; these percentages will add up to 100. (The **% of Tot. Errors** option is active if there is an X in the check box.) The pie chart in the center of the window provides a graphical view of the selected percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.



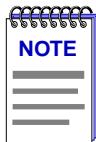
If you reset your device, you must first close, then re-open the Statistics window to refresh peak values.

Frame Size (Bytes) Packets

The Frame Size (Bytes) Packets fields indicate the number of packets (including error packets) processed by the network segment that were of the noted length, excluding framing bits but including frame check sequence bits. Packet sizes counted are:

- 64
- 65-127
- 128-255
- 256-511
- 512-1023
- 1024-1518

The percentages displayed to the right of the numerical values for these fields indicate what percentage of all packets transmitted on the network segment were of the noted size. Unless the network segment has experienced a significant number of runts and/or giants (which are not counted in this group), these percentages will add up to 100. The pie chart in the center of the window provides a graphical view of the percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.



If you reset your device, you must first close, then re-open the Statistics window to refresh peak values.

Viewing Total, Delta, and Accumulated Statistics

By using the **Total**, **Delta**, and **Accum** radio buttons located at the bottom of each Statistics window, you can choose whether to view the total statistics count (since the last time the device was initialized), the statistics count during the last polling interval, or a fresh accumulation of statistics begun when the **Accum** button was selected. The polling interval is user-configurable; see the *User's Guide* for information on setting polling intervals.

To choose **Total**, **Delta**, or **Accum**:

1. Click on the **Total** radio button; after the completion of the current polling cycle plus one complete polling cycle, the screen will display the total count of statistics processed since the entry was created or since the device was last initialized, whichever is most recent. These totals are updated after each polling cycle.
2. Click on the **Delta** radio button; after the completion of the current polling cycle plus two more polling cycles, the screen will display the count of statistics processed during the last polling interval. These counts will be refreshed after each polling cycle.
3. Click on the **Accum** radio button; after the completion of the current polling cycle plus two more polling cycles, the screen will display a fresh cumulative count of statistics. Note that making this selection does **not** clear device counters; you can still re-select **Total** for the total count since the device was last initialized.

Note that switching the statistics displays among **Total**, **Delta**, and **Accum** does not effect the displayed peak values, as peak values are always **Delta** values.

To temporarily freeze the statistics display, select the **Freeze Stats** option; in this mode, statistics will continue to be collected, but the display will not update. To resume normal updates, click again to de-select the freeze option.

Printing Statistics

The **Print** button located at the bottom of the Statistics window allows you to print the current snapshot of statistical data. When you select **Print**, a standard Windows print window like the sample shown in [Figure 3-2](#) will appear.

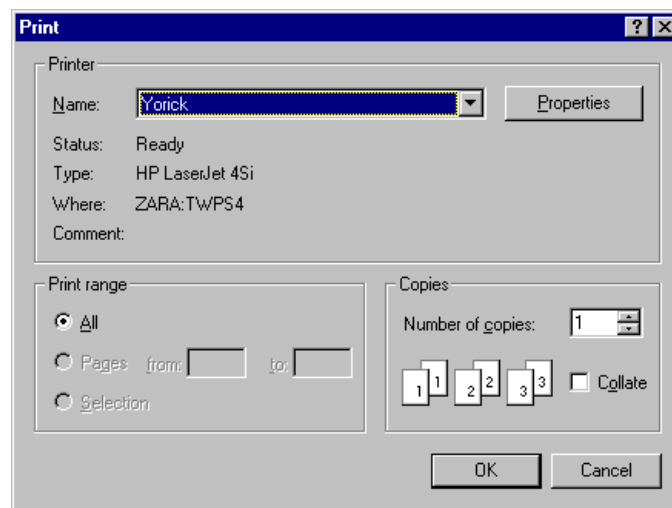
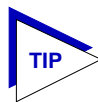


Figure 3-2. Standard Print Window

Adjust printer settings as required, then click **OK**. (For more information on the appropriate printer settings, consult your *Microsoft Windows User's Guide*.)

Interface Statistics

The Interface (IF) Statistics window ([Figure 3-3](#)) provides MIB-II interface statistical information — including counts for both transmit and receive packets, and error and buffering information — for any port interface which does not support RMON, or whose RMON support has been disabled. A color-coded pie chart in the middle of the window lets you graphically view statistics for Unicast, Non-Unicast, Discarded and Error packets.



*This window is also available for all port interfaces — regardless of their level of RMON support or the current administrative status of the RMON Default MIB component — via the I/F Summary window (described in [Chapter 2](#)) or the bridge port menus in the Bridge Status view (see the bridging chapter in your *Tools Guide*).*

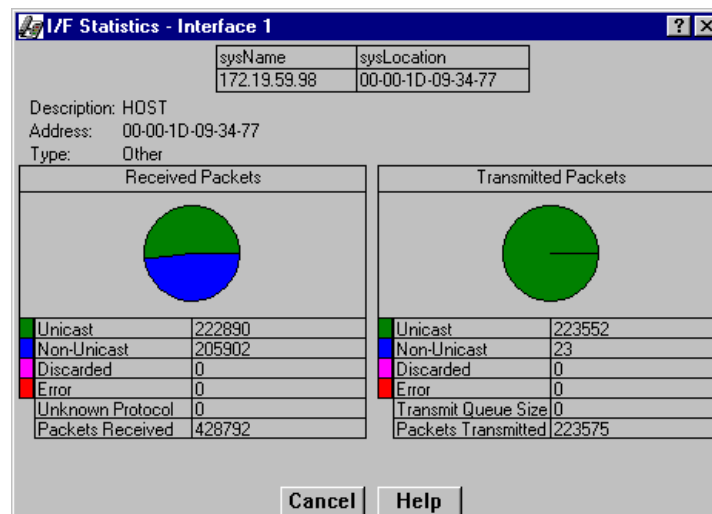


Figure 3-3. Interface Statistics Window

Three informational fields appear in the upper portion of the window:

Description

Displays the interface description for the currently selected port: Ethernet, FDDI, or ATM.

Address

Displays the MAC (physical) address of the selected port.

Type

Displays the interface type of the selected port: ethernet-csmacd, fddi, or atm. Note that there is no type distinction between Ethernet and Fast Ethernet.

The lower portion of the window provides the following transmit and receive statistics; note that the first four statistics are also graphically displayed in the pie charts.

Unicast

Displays the number of packets transmitted to or received from this interface that had a single, unique destination address. These statistics are displayed in the pie chart, color-coded green.

Non-Unicast

Displays the number of packets transmitted to or received from this interface that had a destination address that is recognized by more than one device on the network segment. The non-unicast field includes a count of broadcast packets — those that are recognized by *all* devices on a segment. These statistics are displayed in the pie chart, color-coded dark blue.

Discarded

Displays the number of packets which were discarded even though they contained no errors that would prevent transmission. Good packets are typically discarded to free up buffer space when the network becomes very busy; if this is occurring routinely, it usually means that network traffic is overwhelming the device. To solve this problem, you may need to re-configure your bridging parameters, or perhaps re-configure your network to add additional bridges. Consult the Cabletron Systems *Network Troubleshooting Guide* for more information.

These statistics are displayed in the pie chart, color-coded magenta.

Error

Displays the number of packets received or transmitted that contained errors. These statistics are displayed in the pie chart, color-coded red.

Unknown Protocol (Received only)

Displays the number of packets received which were discarded because they were created under an unknown or unsupported protocol.

Packets Received (Received only)

Displays the number of packets received by the selected interface.

Transmit Queue Size (Transmit only)

Displays the number of packets currently queued for transmission from this interface. The amount of device memory devoted to buffer space, and the traffic level on the target network, determine how large the output packet queue can grow before the SmartSwitch 7000 will begin to discard packets.

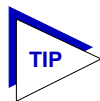
Packets Transmitted (*Transmit only*)

Displays the number of packets transmitted by this interface.

Alarm Configuration

Accessing the Basic and Advanced Alarms windows; creating a basic alarm; creating an advanced alarm; creating events; assigning actions to events; viewing the event log

Through the RMON Alarm and Event functionality supported by your SmartSwitch 7000, you can configure alarms and events (and, where appropriate, actions) for each available interface.



*The Alarm, Event, and Actions windows described in this chapter are identical to those provided via the RMON utility. For more information about other features of RMON, see the **RMON User's Guide**.*

About RMON Alarms and Events

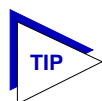
Although Alarms and Events are defined as separate RMON groups, neither one can function properly without the other: you can define an alarm threshold, but if it doesn't point to an event, there will be no indication that the threshold has been crossed; similarly, you can define an event, but unless it is attached to an alarm threshold, it won't be triggered. Each is an essential part of the same notification process: the alarm defines a set of conditions you want to know about, and the event determines the means of letting you know those conditions have occurred.

Events are also an integral part of the filter and packet capture functionality: you can start and stop packet capturing in response to events, or a successful packet capture can generate its own event.

SPECTRUM Element Manager provides two means for configuring RMON alarms: using the Basic Alarms window, you can define both rising and falling alarm thresholds for up to three pre-selected MIB-II variables per interface; based on the options you select, the application automatically creates the necessary events (to log alarm occurrences, generate a trap, or both) and — for devices which support the new Actions MIB — adds the requested actions to those events (to enable or disable bridging at the selected interface).

Using the Advanced Alarms feature, you can define custom alarms for almost any MIB-II or RMON object, as long as it is present in the device firmware and its value is defined as an integer (including counters, timeticks, and gauges). All aspects of these alarms are user-selectable: thresholds can be established on either the absolute or delta value for a variable; events can be configured to create a log, generate a trap, or both; and for devices that support the new Actions MIB, events can also be configured to perform any defined SNMP SET or series of SETs on device objects. The Advanced Alarms feature also allows you to configure any events you wish to use in conjunction with the Packet Capture functionality. (For more information on using the Packet Capture feature, see the **RMON User's Guide**.)

The Basic Alarms feature allows you to assign alarms to any interface type; using the Advanced Alarms feature, you need only be sure to select variables appropriate to the interface — Ethernet for Ethernet, Token Ring for Token Ring, etc. — when defining your alarms.

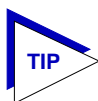


As long as there is at least one Ethernet or Fast Ethernet module installed in your SmartSwitch 7000 chassis, you can use the RMON Alarms feature to configure alarms for MIB objects on FDDI, ATM, and other interfaces that don't specifically support RMON: the Basic Alarms window provides MIB II objects as alarm variables; Advanced Alarm configuration allows you to select any object as an alarm variable, as long as its value is defined as an integer and you assign the correct instance value. See step 5 on [page 4-17](#) and the Note which follows it for more information on assigning the correct instance value to an advanced alarm.

Basic Alarm Configuration

Using the Basic Alarm Configuration application, you can define both rising and falling alarm thresholds for three selected MIB-II objects: ifInOctets, ifInNUcast, and ifInErrors. Because these pre-selected objects are not RMON-specific, you can configure alarms for all interfaces installed in your SmartSwitch 7000 hub — including those, like FDDI, for which no specific RMON statistics currently exist.

In addition to configuring separate rising and falling thresholds, you can also configure your device's *response* to an alarm condition: when a threshold is crossed, the RMON device can create a log of alarm events, send a trap notifying your management workstation that an alarm condition has occurred, or both; you can even configure an alarm to enable or disable bridging on the offending port in response to a rising or falling alarm condition.



If you are familiar with the RMON MIB and/or with the original Alarm and Event functionality provided by SPECTRUM Element Manager (now known as the Advanced Alarm functionality), you will note that the Basic Alarm Configuration window combines the three parts of creating a working alarm — configuring the alarm itself, configuring an event that will announce the occurrence of an alarm (including assigning any actions), and linking the two — into a single step, and handles the details transparently. For more information about the individual steps involved in creating an alarm, see *Advanced Alarm Configuration*, page 4-10.

Accessing the Basic Alarm Configuration Window

To access the RMON Basic Alarm Configuration window:

1. From the Chassis View, click on the appropriate port interface to display the Port menu.
2. Drag down to **Alarm Configuration**, and release. The RMON Basic Alarm Configuration window, [Figure 4-1](#), will appear.

Port Num	If Num	If Type	Status	Log/Trap	Polling Interval	Rising Threshold	Rising Action	Falling Threshold	Falling Action
1	20001	Enet	Enabled	log&trap	45	200	N/A	>>75	N/A
2	20002	Enet	Disabled						
3	20003	Enet	Enabled	trap	30	100	N/A	>>75	N/A
4	20004	Enet	Disabled						
5	20005	Enet	Disabled						
6	20006	Enet	Enabled	log&trap	45	200	N/A	>>75	N/A
7	20007	Enet	Enabled	log&trap	45	200	N/A	>>75	N/A
8	20008	Enet	Disabled						
9	20009	Enet	Enabled	log	30	100	N/A	>>50	N/A

Interval (sec) :
 Alarm : ☐ Log ☐ Send Trap
 Community :
 Rising Threshold :
 Rising Action : ☐ Enable Port ☐ Disable Port ☐ None
 Falling Threshold :
 Falling Action : ☐ Enable Port ☐ Disable Port ☐ None

Figure 4-1. RMON Basic Alarm Configuration Window

When the window is first launched, no interfaces will be selected, and the **Apply**, **Disable**, and **View Log** buttons will be grayed out: **Apply** and **Disable** will activate when an interface is selected; **View Log** will activate when an interface which has experienced an alarm event is selected. The presence of an event log is indicated by the double greater-than sign (>>) displayed to the left of the threshold value that was crossed.

Viewing Alarm Status

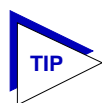
The Basic Alarm Configuration window contains all the fields you need to configure one or more of the three basic alarms available for each interface installed in your RMON device:

Kilobits — Total Errors — Broadcasts/Multicasts

Use these fields at the top of the window to change the alarm type whose status is displayed in the list box. For example, if the **Kilobits** option is selected, the information in the list box pertains to the status of the Kilobits alarm type for each installed interface. Before you configure an alarm or alarms, be sure the appropriate option is selected here.

The available alarm variables are:

- **Kilobits** (*ifInOctets*) — tracks the number of octets of data received by the selected interface. Note that this value has been converted for you from octets (or bytes) to kilobits (or units of 125 bytes); be sure to enter your thresholds accordingly. For example, to set a rising threshold of 1250 octets, enter a threshold value of 10; to set a falling threshold of 625 octets, enter a threshold value of 5.
- **Total Errors** (*ifInErrors*) — tracks the number of error packets received by the selected interface.
- **Broadcast/Multicast** (*ifInNUcast*) — tracks the number of non-unicast — that is, broadcast or multicast — packets received by the selected interface.



Note that the three pre-selected alarm variables are all MIB II variables; this allows you to configure alarms for any installed interface — even those for which no specific RMON statistics yet exist.

Port Number

Provides a sequential indexing of the interfaces installed in your RMON device.

IF Number

Displays the interface number assigned to each available interface. Interfaces installed in a SmartSwitch 7000 chassis are indexed according to an XXXXY scheme, where X = the slot number in which the module containing the port resides, times 10,000; and Y = the physical index assigned to the port. For example, an interface number of 30002 would refer to port 2 on the module installed in slot 3 of the chassis.

IF Type

Displays each interface's type: FDDI, Ethernet, Token Ring, or ATM. Note that there is no type distinction between standard Ethernet and Fast Ethernet.

Status

Displays the current status of the selected alarm type for each interface: Enabled or Disabled. Remember, this status refers only to the alarm type which is selected at the top of the window; each of the other two alarm types can have different states.

Log/Trap

Indicates whether or not each alarm has been configured to create a silent log of event occurrences and the alarms that triggered them, and whether or not each alarm has been configured to issue a trap in response to a rising or falling alarm condition. Possible values are **log**, **trap**, **log&trap**, or **none**.

Polling Interval

Displays the amount of time, in seconds, over which the selected alarm variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds (described below). You can set any interval from 1 to 65,535 seconds.

Rising Threshold

Displays the high threshold value set for the selected alarm variable. Values used to compare to the thresholds are relative, or **delta** values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Rising Action

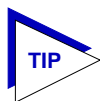
Indicates whether or not a rising alarm occurrence will initiate any actions in response to the alarm condition: **Enable** if bridging will be enabled at the selected interface in response to a rising alarm, **Disable** if bridging will be disabled at the selected interface in response to a rising alarm, and **None** if no actions have been configured for the selected alarm. Note that the Action fields will be unavailable for devices configured to operate in SecureFast switching mode.

Falling Threshold

Displays the low threshold value set for the selected alarm variable. Values used to compare to the thresholds are relative, or **delta** values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Falling Action

Indicates whether or not a falling alarm occurrence will initiate any actions in response to the alarm condition: **Enable** if bridging will be enabled at the selected interface in response to a falling alarm, **Disable** if bridging will be disabled in response to a falling alarm, and **None** if no actions have been configured for the selected alarm. Note that the Action fields will be unavailable for devices configured to operate in SecureFast switching mode.



*Before you decided whether or not to assign an action to a rising or falling alarm, it is important to understand something about the hysteresis function built in to the RMON alarm functionality. See **How Rising and Falling Thresholds Work**, [page 4-26](#), for more information.*

The remainder of the window fields provide the means for configuring alarms for each available interface. Note that the information provided in this screen is static once it is displayed; for updated information, click on **Refresh**. Adding or modifying an alarm automatically updates the list.

Creating and Editing a Basic Alarm

The editable fields at the bottom of the Basic Alarm Configuration window allow you to configure alarm parameters for each available interface. These fields will display the parameters used for the most recently configured alarm (no matter which interfaces are selected in the list box); this allows you to set the same parameters on multiple interfaces with a single set. Hold down the **Shift** key while clicking to select a contiguous group of interfaces; use the **Ctrl** key to select any interfaces. To display the alarm parameters for a specific interface, double-click on that interface.

Note that there is no specific “Enable” function; simply configuring thresholds and/or actions for an alarm and applying those changes enables the alarm. For more information on disabling an alarm, see **Disabling a Basic Alarm**, [page 4-8](#).

To configure an alarm:

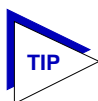
1. At the top of the window, click to select the variable to be used for your alarm: **Kilobits**, **Total Errors**, or **Broadcast/Multicast**. The display in the list box will reflect the current status at each interface of the alarm type you have selected.
2. In the list box, click to highlight the interface (or use **shift-click** or **ctrl-click** to select multiple interfaces) for which you would like to configure an alarm for the selected variable. Note that the editable fields will display the parameters assigned to the most recently set alarm; however, any changes you make in these fields will be set to *all* selected interfaces.
3. In the **Interval** field, enter the amount of time, in seconds, over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. You can assign any interval from 1 to 65,535.
4. In the **Alarm** field, click to select one or both of the following options:
 - a. Select **Log** if you wish to create a silent log of alarm occurrences.
 - b. Select **Trap** if you want your device to issue a trap in response to each alarm occurrence.



In order for the trap selection to work properly, your SmartSwitch 7000 must be configured to send traps to your network management station. This is accomplished via Local Management and the Trap Table; consult your device hardware manual for more information.

*If you are monitoring a variable you consider to be critical, we do not recommend that you select **Trap** as the only event response; if a trap is lost due to a collision or other transmission problem, it will not be re-sent.*

5. Any value you enter in the **Community** field will be included in any trap messages issued by your SmartSwitch 7000 in response to the alarm(s) you are configuring; this value is also used to direct traps related to this alarm to the appropriate management workstation(s):
 - a. **If you enter a value in this field**, traps related to the associated alarms will only be sent to the network management stations in the device's trap table *which have been assigned the same community name* (and for which traps have been enabled). Any IP addresses in the device's trap table which have *not* been assigned the same community string, or which have been assigned no community string, will not receive traps related to the alarm(s) you are configuring.
 - b. **If you leave this field blank**, traps related to the associated alarms will be sent to any network management stations which have been added to the device's trap table, and for which traps have been enabled — regardless of whether or not those IP addresses have been assigned a community name in the Trap Table.



For more information about configuring the SmartSwitch 7000's Trap Table, consult your Local Management documentation. (Remember, no traps will be sent by your 7C0x at all unless its Trap Table has been properly configured!)

6. Click in the **Rising Threshold** field; enter the high threshold value for this alarm. Remember, compared values are always relative, or delta values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Remember, too, when configuring a **Kilobits** alarm, SPECTRUM Element Manager converts octets into kilobits (units of 125 bytes, or octets) for you; for example, to set a rising threshold of 1250 octets, enter a threshold value of 10.

7. In the **Rising Action** field, click to select the action you want your device to take in response to a rising alarm: Enable Port, Disable Port, or None. Note that this action enables and disables only *bridging* at the specified port, and not the interface itself.

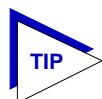
For more information on how actions are triggered, see **How Rising and Falling Thresholds Work**, [page 4-26](#).

8. Click in the **Falling Threshold** field; enter the low threshold value for this alarm. Remember, compared values are always relative, or delta values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Remember, too, when configuring a **Kilobits** alarm, SPECTRUM Element Manager converts octets into kilobits (units of 125 bytes, or octets) for you; for example, to set a falling threshold of 625 octets, enter a threshold value of 5.

9. In the **Falling Action** field, click to select the action you want your device to take in response to a falling alarm: Enable Port, Disable Port, or None. Note that this action enables and disables only *bridging* at the specified port, and not the interface itself.

For more information on how actions are triggered, see **How Rising and Falling Thresholds Work**, [page 4-26](#).



Remember, the Actions fields will be grayed out for devices configured to operate in SecureFast switching mode, as there is no active bridging component on those interfaces.

10. Click **Apply** to set your changes. If you have made any errors in configuring alarm parameters (using an invalid rising or falling threshold, for example, or neglecting to supply a polling interval), either an error window with the appropriate message will appear, or a beep will sound and the cursor will blink in the field which contains the error. Correct the noted problem(s), and click **Apply** again.

Once you click **Apply**, the configured alarm parameters will be set for every selected interface, and the alarms will automatically be enabled; the list box display will also refresh to reflect these changes.

To configure additional alarms, or alarms of a different type, select the appropriate alarm variable at the top of the window, highlight the appropriate interface(s), and repeat the procedures outlined above.

Disabling a Basic Alarm

Using the **Disable** button at the bottom of the window actually performs two functions: it both disables the alarm and deletes the alarm entry (and its associated event and action entries) from device memory to help conserve device resources. In the list box display, the parameters for any “disabled” alarm are automatically reset to their default values.

To disable an alarm:

1. In the top of the window, click to select the variable for which you wish to disable an alarm: **Kilobits**, **Total Errors**, or **Broadcast/Multicast**.
2. In the list box display, click to highlight the interface(s) for which you wish to disable the selected alarm type. (Remember, you can use **shift-click** to select a sequential group of interfaces, or **ctrl-click** to select any group of interfaces.)
3. Click on **Disable**. The selected alarm type on the selected interface(s) will be disabled, and the list box display will refresh to reflect those changes.

Viewing the Basic Alarm Log

If you have selected the “log” response for an alarm, and that alarm’s rising and/or falling threshold has been crossed, the Basic Alarms application will create a log of alarm occurrences. If a threshold has been crossed, it will be proceeded in the interface list box display by a double greater-than sign (>>). Clicking to select an interface which is so marked will activate the **View Log** button; selecting the **View Log** button will launch the appropriate Basic Alarm Log, [Figure 4-2](#). (Note that selecting more than one interface — even if all selected interfaces have experienced alarm conditions — will inactivate the **View Log** button; you can only view a single alarm log at a time.)

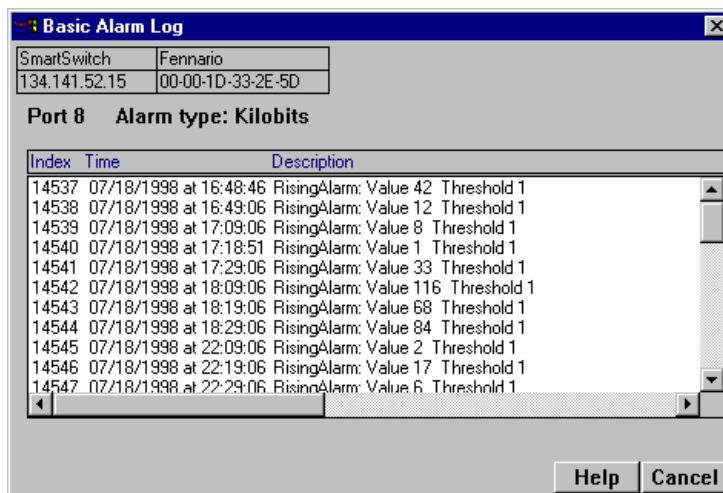
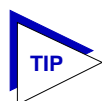


Figure 4-2. Basic Alarm Log

The top portion of the Basic Alarm Log window contains the device information boxes, as well as the Port Number assigned to the interface that experienced the alarm condition and the type of alarm that was triggered; the remainder of the window contains the following information about each alarm occurrence:

Index	This index number uniquely identifies each <i>occurrence</i> of a rising or falling event. Note that, since the alarm whose log is displayed in Figure 4-2 experienced both rising and falling alarms, there are two sets of event indices: one which identifies each instance of the rising alarm, and one which identifies each instance of the falling alarm.
-------	--



*For more information about the relationship between rising and falling alarms and the hysteresis function that controls the generation of alarm events, see **How Rising and Falling Thresholds Work**, [page 4-26](#).*

Time	Indicates the date and time of each event occurrence.
Description	Provides a detailed description of the condition which triggered the alarm, including whether it was a Rising or Falling alarm, the Value which triggered the alarm, and the configured Threshold that was crossed.

Each log will hold only a finite number of entries, which is determined by the resources available on the device; when the log is full, the oldest entries will be replaced by new ones.

Advanced Alarm Configuration

The Basic Alarm Configuration window provides a quick and easy way to set up some basic alarms for all of the interfaces installed in your SmartSwitch 7000 chassis. However, if you prefer more control over the parameters of the alarms you set (as well as their associated events and actions) and/or a wider array of choices for each variable, the Advanced Alarm feature provides a powerful and flexible means for configuring alarms, events, and actions to suit your particular networking needs.

Accessing the RMON Advanced Alarm/Event List

To access the RMON Advanced Alarm/Event List window:

1. From the Chassis View, click on the appropriate port interface to display the Port menu; drag down to **Alarm Configuration**, and release.
2. In the Basic Alarm Configuration window, click on Advanced; the RMON Advanced Alarm/Event List window, [Figure 4-3](#), will appear.

Advanced Alarm/Event

Fred Can't Fish (still sysLocation)
172.19.59.54 00-00-1D-1E-89-CC

ALARMS WATCH Refresh Create/Edit Delete

Index	Interval	Sample	LoThreshd	Event#HiThreshd	Event#Status	Alarm Variable
1	00:01:00	absolute 0	0	0	0	valid ifInOctets.20008
2	00:01:00	delta 75	1	200	1	valid ifAdminStatus.20
3	00:01:00	absolute 50	0	100	0	valid ifInOctets.20008

EVENTS WATCH Refresh Create/Edit Delete

Index	LastTime	Type	Description
1	--none--	log	High Threshold Exceeded
2	--none--	log	Low Threshold Exceeded
3	--none--	log	Packet Match Occurrence

Event Log Help Cancel

Figure 4-3. The RMON Advanced Alarm/Event List Window



Neither the Alarms or Events list is interface-specific; both will be displayed the same for every interface.

Note, too, that alarms and events which have been configured via the Basic Alarms window are not displayed in and cannot be accessed or edited from the Advanced Alarm/Event List window.

The top portion of the window displays the usual device information boxes; the remainder of the window contains the Alarms Watch and Events Watch lists, and the command buttons that allow you to create, edit, and delete entries in those lists, or refresh the display.

The fields in the Alarms Watch display include:

Index

The index is a number that uniquely identifies each alarm. Index numbers are user-defined; you can use any indexing scheme that works for you. These numbers are permanently assigned to their associated alarms; however, index numbers made available by the deletion of existing alarms can be assigned to new alarms, as needed. Note that indices 2000 to 3999 are reserved and unavailable.


Interval	Indicates the amount of time, in seconds, over which the selected variable will be sampled. At the end of the interval, the sample value is compared to both the rising and falling thresholds configured for the alarm.
Sample	Indicates whether the sample value to be compared to the thresholds is an absolute , or total value — that is, the total value counted for the selected variable during the interval — or a relative, or delta value — the difference between the value counted during the current interval and the value counted during the previous interval.
LoThrshld	Indicates the set value for the low, or falling threshold.
Event #	Indicates the event index number that the falling threshold points to: this is the event that will be triggered if the falling threshold is met or crossed. If the value for this field is zero, no event will be triggered.
HiThrshld	Indicates the set value for the high, or rising threshold.
Event #	Indicates the event index number that the rising threshold points to: the event that will be triggered if the rising threshold is met or crossed. If the value for this field is zero, no event will be triggered.
Status	Indicates the status of the alarm: valid, invalid, or underCreation. An alarm that is invalid is not functional; it may be referring to a MIB component that is inactive (such as the Hosts component), not present, or unreachable, or it may have been deleted by software but not yet removed from memory at the device. An alarm that is underCreation is in the process of being configured (possibly by another management station), and should not be modified until its status is valid; if it never reaches valid status, it will eventually be removed.
Alarm Variable	Indicates the variable that is being watched. You can use the scroll bar, if necessary, to view the complete name.

Note that the information provided in this screen is static once it is displayed; for updated information, click on **Refresh**. Adding or modifying an alarm automatically updates the list.

The fields in the Events Watch display include:


Index	This is a number that uniquely identifies an entry in the event table; an index number is assigned when an event is created. These numbers are extremely important, as they are the means by which an event is associated with an alarm or a packet capture filter. As with alarms, these index numbers are user-defined and can be assigned according to any indexing scheme that works for you.
-------	---

	Index numbers are permanently assigned to their associated events; however, numbers made available by the deletion of existing events can be assigned to new events, as needed. Note that indices 2000 to 4999 are reserved and unavailable.
LastTime	Indicates the last time this event was triggered. Note that this information is static once it is displayed, and the LastTime field will not be updated unless you close, then open, the Alarms/Events window, or click on Refresh .
Type	Indicates the type of response that will be generated if the event is triggered: log, trap, or log & trap. A type of “none” indicates that occurrences of the event will not be logged and no trap will be sent; however, note that this field does not indicate whether or not there are any actions associated with the selected event.
Description	This is a user-defined text description used to identify the event and/or the alarm or packet capture that triggers it.

The  button at the bottom of the screen provides access to the log which lists the occurrences of an event.

Note that the information provided in this screen is static once it is displayed; for updated information, click on **Refresh**. Adding or modifying an event automatically updates the list.

Creating and Editing an Advanced Alarm

The Create/Edit Alarms window ([Figure 4-4](#), following page) allows you to both create new alarms and edit existing ones. When you click on the  button in the Alarms Watch list, the Create/Edit Alarms window will display the parameters of the alarm which is currently highlighted in the list. (If no alarms have yet been configured, a set of default parameters will be displayed.) All of these parameters are editable: to change an existing alarm, edit any parameter *except* the Index value; to create an entirely new alarm, simply assign a new Index number. The ability to assign index numbers allows you to quickly and easily create a number of similar alarms without having to close, then re-open the window or re-assign every parameter.

Note, too, that the main Alarm/Event window remains active while the Create/Edit Alarm window is open; to edit a different alarm (or use its settings as the basis of a new alarm), simply double-click on the alarm you want to use in the main Alarms Watch list, and the Create/Edit Alarm window will update accordingly.

To configure an alarm:

1. **If you wish to modify an existing alarm** or create a new alarm based on the parameters of an existing one, be sure the alarm of interest is highlighted in the Alarms Watch list, then click on **Create/Edit** at the top of the Alarms Watch portion of the RMON Advanced Alarm/Event List. The Create/Edit Alarms window, [Figure 4-4](#), will appear.

If you wish to create an entirely new alarm, it doesn't matter which existing alarm (if any) is highlighted when you open the Create/Edit Alarms window; although the window will, by default, display the parameters of whichever alarm is currently selected, all parameters are editable and can be configured as desired.



Whether you are modifying an existing alarm or creating a new one is determined solely by the assignment of the Index number: if you assign a previously unused index number, a new alarm instance will be created; if you use an existing index number, its associated alarm will be modified.

Create / Edit Action: 172.19.59.54

Fred Can't Fish (still sysLocation)
172.19.59.54 00-00-1D-1E-89-CC

Event: **1** High Threshold Exceeded

Description:

Variable:

Instance:

Value:

Action Table:

Variable	Instance	Value

Variable Selection:

*List Find-> rmon=1.3.6.1.2.1.16

- mib-2
 - system
 - interfaces
 - at
 - ip
 - icmp
 - tcp
 - udp
 - egp
 - transmission
 - snmp
 - appletalk
 - ospf
 - rmon

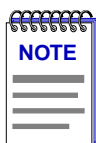
Refresh Add Delete Help Cancel

Figure 4-4. The RMON Create/Edit Alarms Window

2. In the **Owner** text box, enter some appropriate text designation for this alarm, if desired; you may want to use the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the creator of the alarm. Since any workstation can access and change the alarms you are setting in your SmartSwitch 7000, some owner identification can prevent alarms from being altered or deleted accidentally. The default

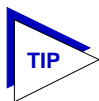
value provided is SPEL — <IP address> <(hostname)> <date> <time>, where <IP address> and <(hostname)> refer to the workstation that created the alarm and <date> and <time> reflect the date and time of the alarm's creation.

3. **If you are creating a new alarm**, use the **Index** field to assign a unique, currently unused index number to identify the alarm. Clicking on the **Index** button will automatically assign the lowest available number; you can also click directly in the text box and assign any value you want between 1 and 1,999 and 4,000 and 9,999 (indices 2000 to 3999 are reserved and unavailable).



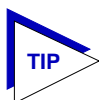
*Clicking on the **Index** button to select the next available index number will replace the current Owner string with the default value described above; if the default value is already in place, the date and time will be updated.*

If you wish to modify an existing alarm, enter the appropriate index value, or double-click on the alarm of interest in the Alarms Watch list (in the main Alarm/Event window).



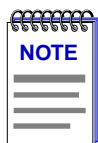
Remember, the only thing that determines whether you are modifying an existing alarm or creating a new one is the assignment of the index number; be sure to assign this value appropriately.

4. To select the **Variable** to be used for your alarm, use the MIBTree panel provided on the right side of the window. (For more information about how to use the MIBTree utility, see the **Tools Guide**.) The display will default to the top of the tree (labeled Internet); there are two ways to locate and/or assign the correct variable:
 - a. If you know the exact name of the OID whose value you wish to track (including its capitalization), simply enter the name in the **Alarm Variable** field; to verify that you have entered the name correctly, click on **Find->** to move the MIBTree display to that OID. (If MIBTree display does not adjust to show the OID you've entered, you've entered the name incorrectly; remember, case does count!)
 - b. Use the scroll bars and click to open the appropriate folders in the MIBTree panel to locate the object you wish you use; click to select it in the panel, and its name will automatically be entered in the **Alarm Variable** field.



*If you don't know the exact spelling of the OID you wish to use for your alarm variable, and you can't find it by searching through the tree, use the MIBTree utility's Find feature to locate the OID and determine its exact spelling (and tree location). For more information on the MIBTree utility and its Find capabilities, see the **Tools Guide**.*

Almost any RMON or MIB-II object can be used as an alarm variable as long as it is resident in the device firmware and its value is defined as an integer (including counters, timeticks, and gauges). If you select an invalid object (i.e., one whose value is not an integer), the message “!!Can’t set alarm on this type!!” will display in the Alarm Variable field.

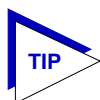


*If you select an object which is not resident in the device firmware, you will receive a “Set Failed; ensure variable is readable” message when you try to set your alarm by clicking on **Apply**. If you are unsure just which objects are resident on your device, and you find yourself receiving a lot of “Set Failed” messages, you can use the MIBTree utility (accessed from the main console window menu bar or from a device Chassis View) to determine which objects are and are not part of your device’s firmware — simply query the object you are interested in; if the query response comes back empty, the object is not present (make sure you are using the appropriate community name when making a query, or you will get no response).*

5. Once you have selected the object you wish to use for your alarm variable, you must assign the appropriate instance value in the **Alarm Instance** field. Most RMON objects are instantiated by the index number assigned to the table in which they reside; for example, if you wish to set an alarm on an object located in an RMON Statistics table, you can determine the appropriate instance by noting the index number assigned to the table that is collecting data on the interface you’re interested in. In the case of the default tables, *index* numbers often mirror *interface* numbers; however, if there are multiple default tables per interface, or if additional tables have been created, this may not be true. (Table index numbers are assigned automatically as table entries are created; no two tables — even those on different interfaces — will share the same table index number.)

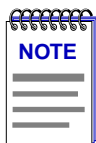
If you have selected an object from a table which is indexed by some other means — for example, by ring number — you must be sure to assign the instance accordingly. If you’re not sure how a tabular object is instantiated, you can use the MIBTree utility (described in the **Tools Guide**) to query the object; all available instances for the object will be displayed. (Host and matrix table objects — which are indexed by MAC address — require special handling; see the Note which follows this step.)

If you have selected an object which is *not* part of a table, you must assign an instance value of 0.



*You can use the MIBTree panel to determine which objects are tabular and which are not: objects which are part of a table will descend from a **blue** folder (which will have a “T” on it, and a name which will almost always include the word “table”); objects which are not will descend directly from a **yellow** folder. (Note: There may be one or more yellow folders in between the blue folder which contains the table and the leaf object you wish to use; however, those objects are still part of the table.)*

Be sure you define your instance values carefully; if you neglect to set the instance correctly, you will receive the “Set failed; ensure variable is readable” error message when you click **Apply** to set your alarm.



If you wish to set an alarm on an object whose instance is non-integral — for example, a Host Table object indexed by MAC address — or on an object with multiple indices, like a Matrix Table entry (which is indexed by a pair of MAC addresses), you must follow certain special procedures for defining the instance. For these OIDs, the instance definition must take the following format:

table index.length(in bytes).instance(in decimal format)

For the first byte of the instance, you must use the index number of the **table** which contains the OID you want to track. For example, to set an alarm on an object in the Host Table, define the first byte of the instance as the index number assigned to the specific Host Table you want to check. These index numbers are assigned automatically as the table entries are created; no two tables — even if they are on different interfaces — will share the same table index number.

Second, you must specify the length, in bytes, of the index you will be using. Again, in the case of an object in the Host Table, that value would be 6, since Host Table entries are indexed by MAC address — a six-byte value.

Finally, you must specify the index itself, in **decimal** format. In the case of a MAC address, that means you must convert the standard hexadecimal format to decimal format. To do this, simply multiply the first digit of the two-digit hex number by 16, then add the value of the second digit. (For hex values represented by alphabetical characters, remember that a=10, b=11, c=12, d=13, e=14, and f=15.) A hex value of b7, for instance, is represented in decimal format as $16 \times 11 + 7$, or 183.

So, for example, the instance for an object in the Hosts group might read as follows:

2.6.0.0.29.170.35.201

where 2=the host table index; 6=the length in bytes of the index to follow; and 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9.

For objects with multiple indices — such as objects in a matrix table — you must add additional length and index information to the instance definition, as illustrated below:

3.6.0.0.29.170.35.201.6.0.0.29.10.20.183

where 3=the matrix table index; 6=the length in bytes of the index to follow; 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9; 6=the length in bytes of the next index; and 0.0.29.10.20.183=the decimal format for MAC address 00-00-1d-0a-14-b7.

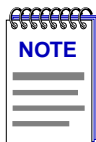
Additional instance issues may exist for FDDI objects; if you're unsure how to assign an instance, use the MIBTree utility to query the object of interest, and note the appropriate instancing on the returned values.

6. In the **Alarm Interval** field, enter the amount of time over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. There is no practical limit to the size of the interval (as the maximum value is 24,855 days 3 hours 14 minutes and 7 seconds — over 68 years!); the default value is 1 minute.
7. Since the first sample taken can be misleading, you can use the selections in the **Startup Alarm** box to disable either the rising or the falling threshold for that sample only. If you would like to exclude the falling alarm, select the **Rising** option; the first sample taken will only generate a rising alarm, even if the sample value is at or below the falling threshold. To exclude the rising alarm, select the **Falling** option; the first sample will then only generate a falling alarm, even if the sample value is at or above the rising threshold. If you wish to receive both alarms as appropriate, select the **Both** option.
8. Use the selections in the **Sample Type** box to indicate whether you want your threshold values compared to the total count for the variable during the interval (**Absolute**), or to the difference between the count for the current interval and the count for the previous interval (**Delta**). Make sure you have set your thresholds accordingly.
9. Click in the **RisingThreshold** field; enter the high threshold value for this alarm.
10. There are two ways to assign an event to your rising threshold: click in the **RisingEventIndex** text box and enter the number of the event you would like to see triggered if the rising threshold is crossed; or use the Events Watch list in the main Alarm/Event window to highlight the desired event, then click on the **Rising Event Index** button. Be sure you assign the number of a valid event or there will be no response if the selected variable meets or crosses this threshold; assigning an index of zero effectively disables the threshold, as there will be no indication that it has been crossed.

For more information on how events are triggered, see **How Rising and Falling Thresholds Work**, [page 4-26](#).

11. Click in the **FallingThreshold** field; enter the low threshold value for this alarm.
12. There are two ways to assign an event to your falling threshold: click in the **FallingEventIndex** text box and enter the number of the event you would like to see triggered if the falling threshold is crossed; or use the Events Watch list in the main Alarm/Event window to highlight the desired event, then click on the **Falling Event Index** button. Again, be sure you assign the number of a valid event or there will be no response if the selected variable meets or crosses this threshold; assigning an index of zero effectively disables the threshold, as there will be no indication that it has been crossed.

For more information on how events are triggered, see **How Rising and Falling Thresholds Work**, [page 4-26](#).



There is no limit to the number of alarms that may be assigned to the same event.

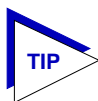
13. Click **Apply** to set your changes. If you have made any errors in configuring alarm parameters (using an invalid value in any field, leaving a field blank, or selecting an alarm variable which is not resident on the device), an error window with the appropriate message will appear. Correct the noted problem(s), and click **Apply** again.

Note that the window remains open so that you may configure additional new alarms or modify existing ones; remember, you can double-click on any alarm in the Alarms Watch list in the main Alarm/Event window to display its parameters in the Create/Edit Alarm window. When you have finished configuring your alarms, click on **Cancel** to close the window.

Creating and Editing an Event

The Create/Edit Events window (Figure 4-5, page 4-20) — like the Create/Edit Alarms window — allows you to both create new events and edit existing ones. When you click on the **Create/Edit** button in the Events Watch list, the Create/Edit Events window will display the parameters of the event which is currently highlighted in the list. (If no events have yet been configured, a set of default parameters will be displayed.) All of these parameters are editable: to change an existing event, edit any parameter *except* the Index value; to create an entirely new event, simply assign a new Index number. The ability to assign index numbers allows you to quickly and easily create a number of similar events without having to close, then re-open the window or re-assign every parameter.

Note, too, that the main Alarm/Event window remains active while the Create/Edit Event window is open; to edit a different event (or use its settings as the basis of a new event), simply double-click on the event you want to use in the main Events Watch list, and the Create/Edit Event window will update accordingly.

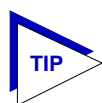


*If the Create/Edit Actions window is also open, it too will update to display the actions associated with the event currently selected in the main Alarm/Event window. See **Adding Actions to an Event**, page 4-23, for more information on the actions feature.*

To configure an event:

1. **If you wish to modify an existing event** or create a new event based on the parameters of an existing one, be sure the event of interest is highlighted in the Events Watch list, then click on **Create/Edit** at the top of the Events Watch portion of the RMON Advanced Alarm/Event List. The Create/Edit Events window, **Figure 4-5**, will appear.

If you wish to create an entirely new event, it doesn't matter which existing event (if any) is highlighted when you open the Create/Edit Events window; although the window will, by default, display the parameters of whichever event is currently selected, all parameters are editable and can be configured as desired.



Whether you are modifying an existing event or creating a new one is determined solely by the assignment of the Index number: if you assign a previously unused index number, a new event instance will be created; if you use an existing index number, its associated event will be modified.

Figure 4-5. The RMON Create/Edit Events Window

2. **If you are creating a new event**, use the **Index** field to assign a unique, currently unused index number to identify the event. Clicking on the **Index** button will automatically assign the lowest available number; you can also click directly in the text box and assign any value you want between 1 and 1,999 and 5,000 and 9,999 (indices 2000 to 4999 are reserved and unavailable).



*Clicking on the **Index** button to select the next available index number will replace the current Owner string with the default value; if the default value is already in place, the date and time will be updated.*

If you wish to modify an existing event, enter the appropriate index value, or double-click on the event of interest in the Events Watch list (in the main Alarm/Event window).



Remember, the only thing that determines whether you are modifying an existing event or creating a new one is the assignment of the index number; be sure to assign this value appropriately.

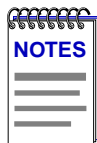
3. Click in the **Description** text box to enter any text description you want to identify the event. This description will appear in the Events Watch window and help you distinguish among the events you have configured.
4. Any value you enter in the **Community** field will be included in any trap messages issued by your SmartSwitch 7000 when this event is triggered; this value is also used to direct traps related to this event to the appropriate management workstation(s):
 - a. **If you enter a value in this field**, traps related to this event will only be sent to the network management stations in the device's trap table *which have been assigned the same community name* (and for which traps have been enabled). Any IP addresses in the device's trap table which have *not* been assigned the same community string, or which have been assigned no community string, will not receive traps related to the alarm(s) you are configuring.
 - b. **If you leave this field blank**, traps related to this event will be sent to any network management stations which have been added to the device's trap table, and for which traps have been enabled — regardless of whether or not those IP addresses have been assigned a community name in the Trap Table.



For more information about configuring your SmartSwitch 7000's Trap Table, consult your Local Management documentation. (Remember, no traps will be sent by your 7C0x at all unless its Trap Table has been properly configured!)

5. You can use the **Owner** text box for administrative or informational purposes; although the text entered here will not appear on any other screens, you may want to use the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the owner of the event. Since any workstation can access and change the events you are setting in your RMON device, some owner identification can prevent events from being altered or deleted accidentally. The default value provided is SPEL — <IP address> <(hostname)> <date> <time>, where <IP address> and <(hostname)> refer to the workstation that created the event and <date> and <time> reflect the date and time of the event's creation.

6. Use the options in the **Event Type** field to define how this event will respond when an associated threshold is crossed:
 - a. Select the **Log** option to create a silent log of event occurrences and the alarms that triggered them. Each event's log can be viewed by clicking on **Event Log** at the bottom of the Alarm/Event window. (See **Viewing an Advanced Alarm Event Log**, page 4-25, for more information.)
 - b. Select **Trap** to instruct the device to send a pair of SNMP traps (one WARNING, one Normal) to the management station each time the event is triggered.

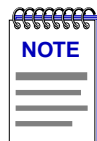


In order for the trap selection to work properly, your SmartSwitch 7000 must be configured to send traps to the management station. This is accomplished via local management; consult your device hardware manual for more information.

*If you are monitoring a variable you consider to be critical, we do not recommend that you select **Trap** as the only event response; if a trap is lost due to a collision or other transmission problem, it will not be re-sent.*

- c. Select both **Log** and **Trap** to both log the event occurrence and generate the traps.

If you select neither option, the event's occurrences will neither be logged nor generate traps; unless the event includes an action or a series of actions, this effectively disables the event (since there will be no indication that it has been triggered).



The Event Type field in the Advanced Alarm/Event List window will display a value of "none" if neither the Log nor the Trap response has been selected; note, however, that this field does not indicate whether or not an event has been configured to perform an SNMP SET or series of SETs via the Actions MIB.

7. For devices which support the proprietary Actions MIB, an **Actions** button will appear in the Create/Edit Events window; using this feature, you can configure an SNMP SET or series of SETs that will be performed automatically when the event is triggered. See **Adding Actions to an Event**, below, for more information.
8. Click **Apply** to set your changes. Note that the window remains open so that you may configure additional new events or modify existing ones; remember, you can double-click on any event in the Events Watch list in the main Alarm/Event window to display its parameters in the Create/Edit Event window (and in the Create/Edit Actions window, if it's open). When you have finished configuring your events, click on **Cancel** to close the window.

Adding Actions to an Event

For devices which support the proprietary Actions MIB, selecting the **Actions** button in the Create/Edit Events window opens the Create/Edit Actions window (Figure 4-6), which allows you to define an SNMP SET or series of SETs that will be performed automatically when the associated event is triggered.

To add an action or actions to an event:

1. In the Create/Edit Events window, click on **Actions**. The Create/Edit Actions window, Figure 4-6 (following page), will appear.



If no **Actions** button appears in the Create/Edit Events window, the selected SmartSwitch 7000 does not support the Actions MIB. For more information about devices which support this MIB, contact Cabletron Systems Technical Support.

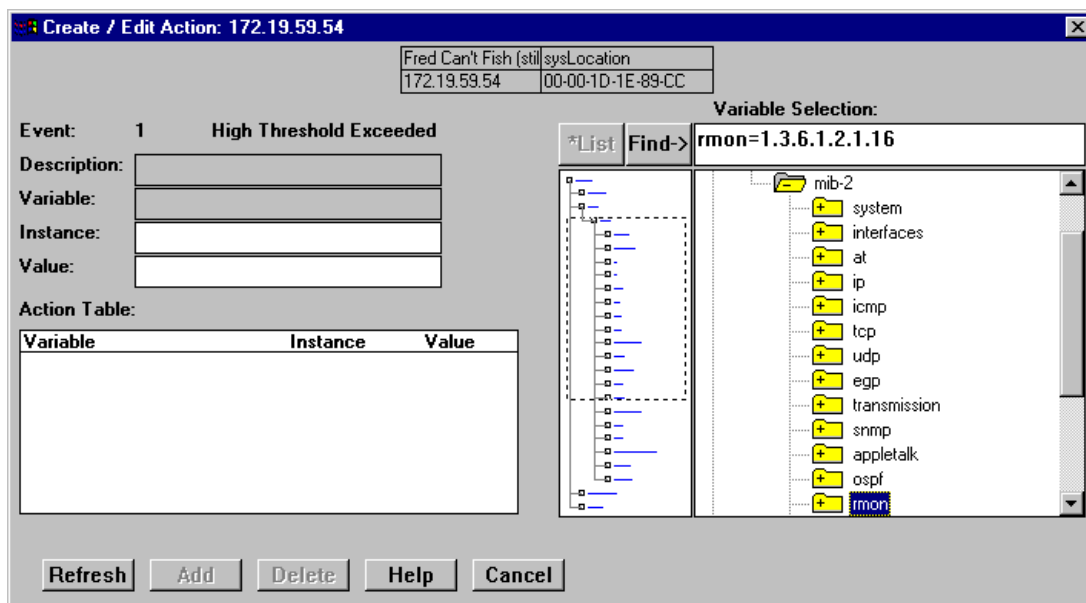
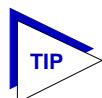


Figure 4-6. The RMON Create/Edit Actions Window

2. The index number and description of the event with which the action or actions will be associated is displayed in the **Event:** field at the top of the window. Information in this field is not editable; to assign actions to a different event, double-click on the correct event in the Events Watch list; both the Create/Edit Events and Create/Edit Actions windows will update accordingly.

3. The **Description** field is not currently editable; future releases of SPECTRUM Element Manager will allow you to assign a descriptive label to each set of actions.
4. To select the **Variable** whose value you wish to SET, use the MIBTree panel provided on the right side of the window. (For more information about how to use the MIBTree utility, see the **Tools Guide**.) The display will default to the top of the tree (labeled Internet); there are two ways to locate and/or assign the correct variable:
 - a. If you know the exact name of the OID whose value you wish to track (including its capitalization), simply enter the name in the **Variable** field; to verify that you have entered the name correctly, click on **Find->** to move the MIBTree display to that OID. (If MIBTree display does not adjust to show the OID you've entered, you've entered the name incorrectly; remember, case does count!)
 - b. Use the scroll bars and click to open the appropriate folders in the MIBTree panel to locate the object you wish you use; click to select it in the panel, and its name will automatically be entered in the **Variable** field.



If you select an invalid OID — that is, one which does not permit write access — the message !Can't set action - not write access!! will be displayed in the Variable field.

*If you don't know the exact spelling of the OID you wish to use for your alarm variable, and you can't find it by searching through the tree, use the MIBTree utility's Find feature to locate the OID and determine its exact spelling (and tree location). For more information on the MIBTree utility and its Find capabilities, see the **Tools Guide**.*

5. Once you have selected the object you wish to set, you must assign the appropriate instance value in the **Instance** field. If you're not sure how the object you wish to set is instanced, you can use the MIBTree utility (described in the **Tools Guide**) to query it; all available instances for the object will be displayed.
6. In the **Value** field, enter the value you wish to set for the selected object. Again, if you're not sure what the valid values are for the variable you wish to set, locate the object in the MIBTree utility and use the **Details** button to obtain more information.
7. Once you've configured your action, click on **Add**; the action will be added to the Action Table list in the lower left corner of the window. Note that the window remains open so that you may configure additional new actions or modify existing ones; selecting on any action in the Action Table will display that action's parameters in the window and make them available for editing. When you have finished configuring your actions, click on **Cancel** to close the window.

Note that the Action Table will update automatically each time an action is added or deleted; use the **Refresh** button to update the table at any time.

Deleting an Alarm, Event, or Action

To delete an alarm, event, or action:

1. In the appropriate window, highlight the alarm, event, or action you wish to remove.
2. Click on **Delete** to remove. A window will appear asking you to confirm your selection; click on **OK** to delete, or on **Cancel** to cancel.

When you delete an event, be sure you edit all alarms that were pointing to that event, and assign a new valid event to those thresholds; note, too, that deleting an event automatically deletes its associated actions, as actions cannot exist in the absence of an association with an event.

Again, as a general rule, we recommend that you do *not* delete an alarm or event of which you are not the owner.

Viewing an Advanced Alarm Event Log

To view the log of occurrences for any event:

1. Highlight the event for which you wish to view the log, then click on **Event Log** at the bottom of the Advanced Alarm/Event List window; the Event Log window, [Figure 4-7](#), will appear.

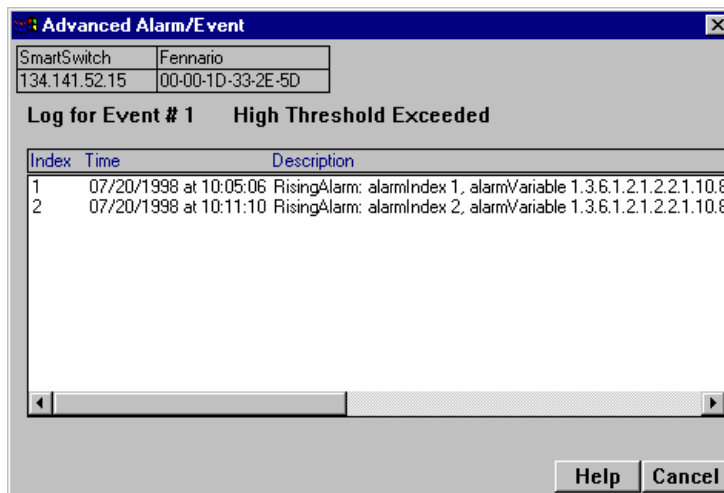


Figure 4-7. The Event Log Window

The top portion of the window contains the device information boxes, as well as the event index number and the event description; the log itself includes the following fields:

Index	This index number is not the <i>event's</i> index, but a separate index that uniquely identifies this <i>occurrence</i> of the event.
Time	Indicates the date and time of each event occurrence.
Description	Provides a detailed description of the alarm that triggered the event: whether it was a rising or falling alarm, the alarm index number, the alarm variable name and object identifier (OID), the alarmSampleType (1=absolute value; 2=delta value), the value that triggered the alarm, the configured threshold that was crossed, and the event description. Use the scroll bar at the bottom of the log to view all the information provided.

Each log will hold only a finite number of entries, which is determined by the resources available on the device; when the log is full, the oldest entries will be replaced by new ones.

How Rising and Falling Thresholds Work

Rising and falling thresholds are intended to be used in pairs, and can be used to provide notification of spikes or drops in a monitored value — either of which can indicate a network problem. To make the best use of this powerful feature, however, pairs of thresholds should not be set too far apart, or the alarm notification process may be defeated: a built-in hysteresis function designed to limit the generation of events specifies that, once a configured threshold is met or crossed in one direction, no additional events will be generated until the opposite threshold is met or crossed. Therefore, if your threshold pair spans a wide range of values, and network performance is unstable around either threshold, you will only receive one event in response to what may be several dramatic changes in value. To monitor both ends of a wide range of values, set up two pairs of thresholds: one set at the top end of the range, and one at the bottom. [Figure 4-8](#) illustrates such a configuration.

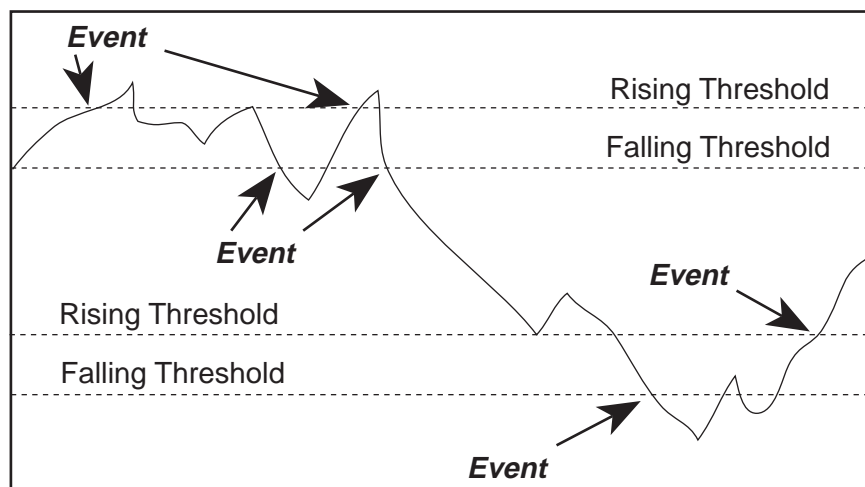
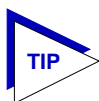


Figure 4-8. Sample Rising and Falling Threshold Pairs



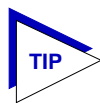
The current version of the Basic Alarms window only allows you to configure a single pair of thresholds for each alarm variable on each interface; be sure to keep this hysteresis function in mind when configuring those threshold values.

FDDI Management

Concentrator configuration; connection policy; station list; concentrator performance

The FDDI menu lets you access windows to view the SmartSwitch 7000's FDDI configuration, connection policy, station list, and performance with respect to Station Management (SMT) entities present on any installed 7F06-02 Network Interface Modules.

SMT provides the system management services for the FDDI protocols, including connection management, node configuration, error recovery, statistics collecting, and management frame encoding. SMT is comprised of various subcomponent functions, including Connection Management (CMT) and Ring Management (RMT); one SMT entity will be present for each ring connected to a 7F06-02 module.

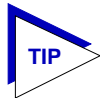


SMT entities installed in the SmartSwitch 7000 hub are indexed according to module and port position in the chassis. For example, if there is one 7F06-02 module installed in the chassis, its rings will be indexed 1 and 2, and the indexes will correspond to the index of the port through which they are connected; if there are two 7F06-02 modules installed, their rings will be indexed 1, 2, 3, and 4, with rings 1 and 2 corresponding to ports 1 and 2 on the module in the lowest numerical slot, and rings 3 and 4 corresponding, respectively, to ports 1 and 2 on the module in the next highest numerical slot.

The windows that provide information about the FDDI rings installed in the SmartSwitch 7000 are:

- **Configuration** — This window displays the current configuration and status of the ring associated with the selected SMT entity.
- **Connection Policy** — This window shows the types of connections between the four FDDI PHY (port) types — A, B, M, and S — that will be allowed by the SMT entity.

- **Station List** — With this window you can see the configuration of the ring on which the SMT entity resides, including number of nodes, node addresses (both Canonical and MAC), node class, and current ring topology.
- **Performance** — This window lets you view the number of frames transmitted and received on the ring as detected by the selected SMT entity, along with error and lost frames, and the number of ring initializations.



*Additional FDDI performance-related statistics are available via the **FDDI Statistics** option on the Chassis View Device menu; see **Chapter 2** for more information.*

To access FDDI information:

1. In the Chassis View window, click on **FDDI**; drag down to select the SMT entity of interest, then right to reveal the FDDI menu ([Figure 5-1](#)).

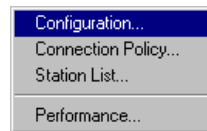


Figure 5-1. The FDDI Menu

2. Drag to select the desired window.

Note that the title bar of each window will display the index number of the SMT entity whose information is being displayed.

Configuration

The Concentrator Configuration window, [Figure 5-2](#), informs you about the configuration and operating state of the FDDI ring associated with the selected SMT entity, and displays parameters relating to ring initialization.

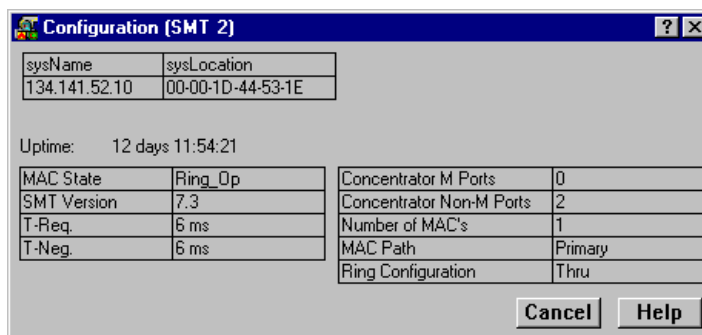


Figure 5-2. The Concentrator Configuration Window

MAC State

This field indicates the current state of the selecting ring's MAC component. (The RMT component of SMT monitors MAC operation and takes actions necessary to aid in achieving an operational ring.) Possible states are:

Not Available	There is no MAC on the FDDI ring associated with the SMT entity.
Ring-Op	The ring is functioning normally. While in this state, the MAC being managed is part of an operational FDDI ring.
Isolated	SMT has just initialized RMT or RMT has entered this state during a path test (trace) after ring beaconing; RMT is not aware of the ring path or state.
Non-Op	The MAC being managed by the selected SMT is participating in ring recovery; the ring is not operational.
Detect	The claim (beacon) process of the FDDI ring protocol has exceeded one second. There may be a problem on the ring; any duplicate address conditions are being detected. In this state, the ring is still alive, but no data is being transmitted.
Non-Op-Dup	The ring is not operational; the address of the MAC under control of the SMT entity has been found to duplicate that of another MAC on the ring. The duplicate address condition prevented ring recovery and initialization after a claim and beacon process. This state will not occur unless you are using locally- administered addresses, as factory-set MAC addresses are guaranteed to be unique.
Ring-Op-Dup	The ring is operational; however, the address of the MAC under control of the SMT entity has been found to duplicate that of another MAC on the ring. Corrective actions will be attempted before the duplicate address

	condition causes ring initialization to fail after the claim and beacon recovery process. Like Non-Op-Dup, this state will not occur unless you are using locally-administered addresses.
Directed	The beacon process did not complete within 7 seconds. The selected SMT has directed the controlled MAC to send beacon frames to notify the other stations that a serious problem exists on the ring, and a Trace state is soon to follow.
Trace	A problem exists on the ring which could not be corrected during the beaconing process, and a Trace has been initiated. During a Trace (or Path Test), the SMT sends a signal that forces its nearest upstream neighbor to remove from the ring and conduct a self-test. If the ring does not recover, each subsequent upstream station will be forced to remove from the ring and conduct self-tests until the problem has been corrected. While the test is being conducted, ring management re-enters the isolated state.

SMT Version

Displays the version number of the Station Management (SMT) entity. SMT provides the system management services for the FDDI protocols, including connection management, node configuration, error recovery, and management frame encoding. SMT frames have a version ID field that identifies the structure of the SMT frame Info field. The version number is included in the SMT frame so that a receiving station can determine whether or not its SMT version is able to communicate with the SMT version of another station. Knowing the version number allows the stations to handle version mismatches. Each FDDI station supports a range of SMT versions. The supported version range is identified within the ietf-fddi MIB by two smtTable attributes: snmpFddiSMTLoVersionId and snmpFddiSMTHiVersionId. If a received frame is not within the supported version range, the frame is discarded.

T-Req. (Requested Target Token Rotation Time)

The token rotation time bid made by the selected SMT entity during ring initialization. Each station detecting that the ring must be initialized begins a claim token process and issues a stream of Claim Frames, which negotiate the value assigned to the Target Token Rotation Time (TTRT). The information field of these frames contains the issuing station's bid for the value of TTRT. Each claiming station inspects incoming Claim frames (from other issuing stations) and either continues its own bid (and removes the competing Claim Frame from the ring) or defers (halts transmission of its own bid and repeats the competing bid) according to the following hierarchy of arbitration:

- A Claim Frame with the lowest TTRT bid has precedence.
- If the values of TTRT are equal, the frame with the longest source address (48 vs. 16 bits) has precedence.

- If both TTRT value and source address length are equal, the frame with the highest address has precedence.

The 7F06-02 is shipped with a default T-Req of 6 msec. T-Req is stored within the MIB in units of nanoseconds (one billionth of a second) rather than milliseconds (one thousandth of a second); SPECTRUM Element Manager converts nanoseconds to milliseconds for display purposes. You can use any SNMP Set Request tool to edit the T-Req value; just remember that you must enter your value in nanoseconds, rather than milliseconds.

T-Neg. (Negotiated)

The winning time negotiated in the ring initialization sequence.

Concentrator M Ports

This field displays the number of Master (M) ports on the device that are associated with the selected SMT entity. A Master port is a port that provides a connection for Single Attachment Station (SAS) devices to the FDDI network. The 7F06-02 does not support M ports, so this field will always display 0.

Concentrator Non-M Ports

This field displays the number of non-Master ports (A, B, or S ports) on the device that are associated with the selected SMT entity. Each 7F06-02 module supports two A / B port pairs; as each pair supports its own ring (and, therefore, its own SMT entity), this field will display 2.

Number of MACs

The number of Media Access Control entities present on the device associated with the selected SMT entity. For the 7F06-02, this number will be 1.

MAC Path

Indicates the configuration of the MAC in respect to the logical ring, as determined by the Connection Management (CMT) portion of SMT. CMT controls the establishment of a media attachment to the FDDI network, the connections with other nodes in the ring, and the internal configuration of the various entities within a node. CMT provides the link confidence test, and specifies a Link Error Monitor (LEM) which monitors active links on a per-link basis to ensure that failing links are detected and, if required, removed from the network. Possible values are:

- **Primary** indicates that the MAC is inserted into the primary path of the currently used FNB ring.
- **Secondary** indicates that the MAC is inserted into the secondary path of the currently used FNB ring.
- **Local** means that the MAC is not inserted into a primary or secondary path of a dual ring, but may be connected to one or more other nodes. This is not a valid value for the 7F06-02.
- **Isolated** means that the MAC has no connection to the ring or other concentrator ports.

- **Not Available** means that there is no MAC on the FDDI ring associated with the selected SMT entity. Again, this state will not occur for the 7F06-02.
- **Unknown** means that device firmware cannot determine the MAC path.
- **?** indicates that SPECTRUM Element Manager cannot determine the MAC path for the selected ring.

Ring Configuration

The current configuration of the MAC and physical layers of the A and B ports.

Connection Policy

The SMT Connection Policy of an FDDI concentrator determines which types of connections are allowed among the four FDDI port types: A, B, M (Master), and S (Slave). FDDI protocol forbids Master—>Master connections; all other connection types are legal, although some are considered to be undesirable.

The Connection Policy window, [Figure 5-3](#), lists potential connection types in a “Reject X-Y” format, where **X** represents a port on the 7F06-02, and **Y** represents the attaching node. An **X** in the checkbox next to a Connection Policy indicates that the connection has been disallowed.

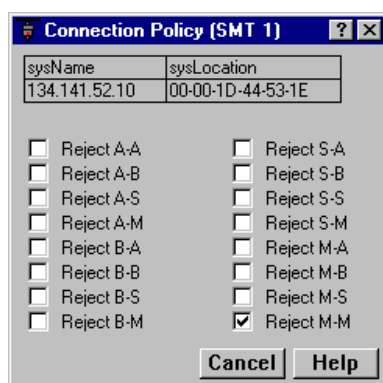


Figure 5-3. The Connection Policy Window

The following table summarizes the FDDI connection rules:

Table 5-1. FDDI Connection Rules

	A	B	S	M
A	V, U	V	V, U	V, P
B	V	V, U	V, U	V, P
S	V, U	V, U	V	V
M	V	V	V	X

V — valid connection

X — illegal connection

U — undesirable (but legal) connection; this requires that SMT is notified.

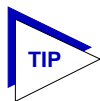
P — valid, but when both A and B are connected to M ports (a dual-homing configuration), only the B connection is used.



Though technically legal under FDDI connection rules, undesirable connections will cause a twisted or wrapped ring.

Each SMT entity maintains its own connection policy; however, when two interfaces attempt to connect, their combined established connection policies dictate the connections that will be allowed. In an attempted connection between two nodes, the most lenient policy will determine whether the connection (as long as it is legal) can be made. For example, if two FDDI nodes attempt an A→A connection, and this connection is not allowed at one FDDI node but allowed at the other, the connection would be accepted. If the connection policy at both nodes disallows the connection, the connection will be rejected.

This is a read-only window; you currently cannot edit the 7F06-02's connection policy via SPECTRUM Element Manager.



You can use any SNMP Set Request or MIB tool to edit the Connection Policy for your device by setting the `fdimibSMTConnectionPolicy` MIB OID (part of the MIBII FDDI Transmission MIB (RFC1512)). `fdimibSMTConnectionPolicy` is simply a 16-bit integer value (ranging from 32768 to 65535) that corresponds to the connection policy (in the "Reject X-Y" format, where X represents a port on the FDDI Switch Module, and Y represents the attaching node).

To set the connection policy for the device, total the bit values corresponding to the desired connection policy according to the table below, and then use your SNMP Set Request or Mib tool to set the value for the appropriate SMT index. For example, to set a connection policy that disallowed the undesirable A-A or B-B connections you would set the `fdimibSMTConnectionPolicy` MIB OID to 32,801: 32,768 (reject M-M, required) + 32 (reject B-B) + 1 (reject A-A).

Policy	Power
reject A-A	2^0 (1)
reject A-B	2^1 (2)
reject A-S	2^2 (4)
reject A-M	2^3 (8)
reject B-A	2^4 (16)
reject B-B	2^5 (32)
reject B-S	2^6 (64)
reject B-M	2^7 (128)
reject S-A	2^8 (256)
reject S-B	2^9 (512)
reject S-S	2^{10} (1,024)
reject S-M	2^{11} (2,048)
reject M-A	2^{12} (4,096)
reject M-B	2^{13} (8,192)
reject M-S	2^{14} (16,384)
reject M-M	2^{15} (32,768 — a permanently set value for this bit)

Station List

The Station List illustrates the configuration of the ring associated with the currently selected SMT entity, including number of nodes on the ring, node addresses (both Canonical and MAC), node class, and ring topology.

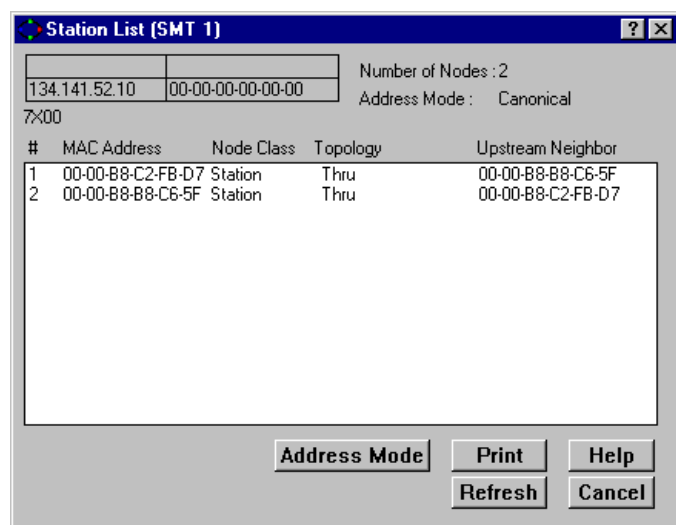


Figure 5-4. The Station List Window

The Station List provides the following information about the ring with which the SMT is currently associated:

Number of Nodes

The number of stations inserted into the FDDI ring with which the SMT entity is currently associated.

Address Mode

Displays the current mode being used to display the addresses of the devices in the Station List. The two possible modes are Canonical (FDDI) or MAC (Ethernet).

To change the current Address Mode, click on the **Address Mode** button at the bottom of the window. The current address mode will change in the Address Mode field and the Stations panel.

Stations Panel

The Stations Panel displays a list of the stations on the ring to which the selected SMT is connected, in ring sequence from the MAC, along with each station's node class and current topology.

Note that the information displayed in the Station List is static once the window is opened; for updated information, click on **Refresh**.

If the number of nodes exceeds the panel size, scroll bars will appear in the list box that will allow you to scroll through the station list to view the node of interest.

Information provided in the Stations Panel includes:

#

An index number assigned to each station that indicates its position on the ring in relation to the monitored SMT's MAC address. The monitored SMT's MAC is always the first entry (1) in the station list.

MAC Address

Displays the 48-bit hardware address — used for universal address assignment — of the node inserted into the ring. These addresses are hardcoded into the device, and are not configurable. The address will appear in Canonical or MAC format, as currently selected.

Node Class

Displays the type of ring device. Possible values are:

Station	Indicates an FDDI node capable of transmitting, receiving, and repeating data.
Concentrator	Indicates an FDDI node that provides attachment points to the ring for stations that are not directly connected to the dual ring.

Topology

Indicates the node's MAC configuration topology.

Upstream Neighbor

Displays hardware address (in Canonical or MAC format, as currently selected) of each node's upstream neighbor.

Performance

The Concentrator Performance window, [Figure 5-5](#), provides graphical and numeric performance statistics for the selected SMT entity, including:

- Transmit Frames
- Receive Frames
- Frame Errors
- Lost Frames
- Ring Ops

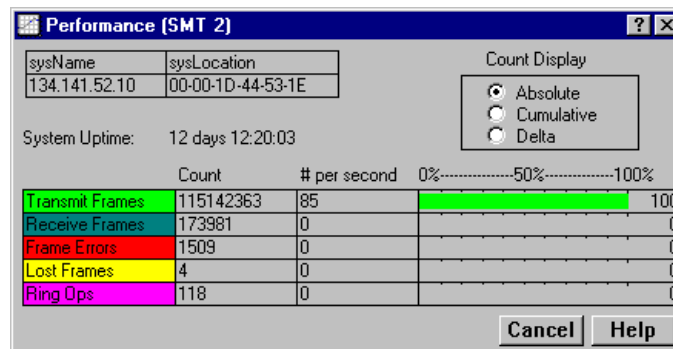


Figure 5-5. Concentrator Performance Window

Statistics are displayed in three ways:

- By count (i.e., the number detected of each for the selected interval).
- By rate (i.e., the number of each per second, as averaged over the selected interval).
- Graphically, as a percentage of each with respect to total network load processed by the selected 7F06-02 interface during the last interval (e.g., a transmit frames rate of 75% during a delta interval indicates that of all frames *processed* by the selected interface, 75% were *transmitted* by that interface).

You can view the concentrator performance for three different intervals:

- **Absolute** — Counts recorded since the SmartSwitch 7000 was last started.
- **Cumulative** — Counts recorded since the Concentrator Performance window was opened.
- **Delta** — Counts recorded during a single polling interval (refer to the *User's Guide* for information on setting the polling interval).

To change the interval, click to select the desired radio button in the **Count Display** panel in the top right hand corner of the window.

Available statistics are:

Transmit Frames

The number of frames transmitted by the MAC associated with the SMT during the chosen interval.

Receive Frames

The number of frames received by the MAC associated with the SMT during the chosen interval.

Frame Errors

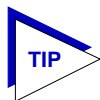
The number of error frames detected by the MAC associated with the SMT during the chosen interval that had not been detected previously by other stations. Error frames may include frames with an invalid Frame Check Sequence (FCS), with data length errors, or with internal errors that prevent the MAC from transferring the frame to the Logical Link Control (LLC) layer.

Lost Frames

The number of frames detected by the MAC associated with the SMT during the chosen interval that have an unknown error, so their validity is in doubt. When the MAC encounters a frame of this type, it increments the Lost Frame counter and strips the remainder of the frame from the ring, replacing it with idle symbols.

Ring Ops

The number of times the ring has entered the “Ring Operational” state from the “Ring Not Operational” state during the selected interval. This counter updates when the MAC informs Station Management (SMT) of a change in Ring Operation status.



*Additional FDDI performance-related statistics are available via the **FDDI Statistics** option on the Chassis View Device menu; see **Chapter 2** for more information.*

ATM Configuration

Viewing connection data; configuring Permanent Virtual Circuits (PVCs); adding and deleting connection entries

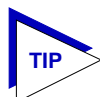
The ATM interface provided by the 7A06-01 NIM module provides the connectivity that allows you to merge ATM network segments with traditional LAN technologies via the SmartSwitch 7000 chassis backplane. Current versions of 9A128-01 firmware use 802.3 VC-based multiplexing for bridging protocols to move PVC traffic between the ATM front panel connection and the switching backplane; future versions will add support for ATM Forum LAN Emulation and Cabletron's SecureFast Switching.

An ATM network uses two types of virtual channels, or circuits: Switched Virtual Circuits, or SVCs, and Permanent Virtual Circuits, or PVCs. SVCs are created and dismantled dynamically on an as-needed basis, and require no management definition; PVCs, however, must be manually configured. The Current ATM Connections window provides the means for accomplishing these configurations.

Accessing the ATM Connections Window

To access the ATM Connections window from the Chassis View:

1. Click on **Device** on the Chassis View menu bar to access the Device menu.
2. Drag down to **ATM Connections**, and release. The Current ATM Connections window, [Figure 6-1](#), will appear.



*Note that the **ATM Connections** option will only be available if at least one 7A06 module is installed in the chassis.*

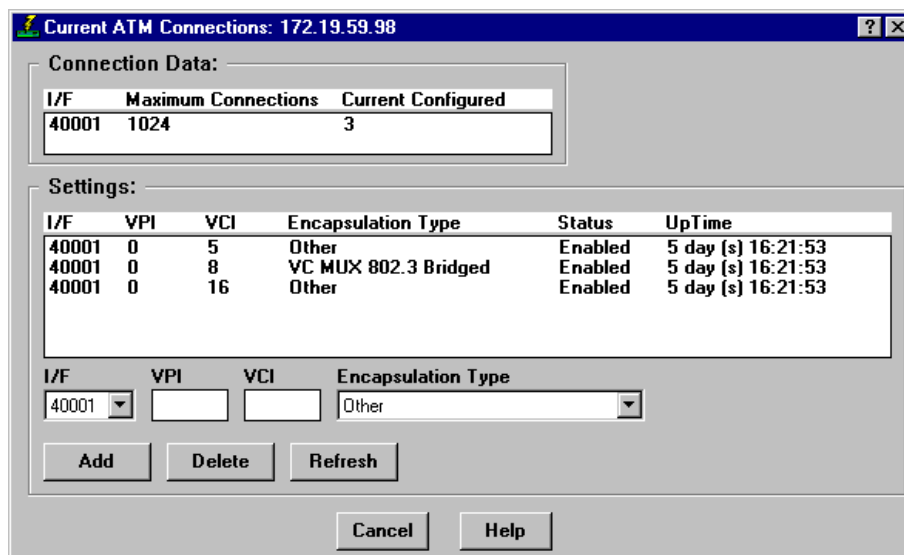


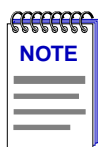
Figure 6-1. The Current ATM Connections Window

The Current ATM Connections window provides the following information about the device's ATM connections:

Connection Data

The Connection Data fields provide the following information about each ATM interface available on the device:

I/F	Displays the index number assigned to each ATM interface installed in the 7C0x chassis. Note that interfaces installed in a 7C0x chassis are indexed following an XXXXY format, where X = the slot number in which the module containing the interface is installed, times 10,000; and Y = the physical index assigned to the port interface on the module. For example, an index of 40001 would refer to port 1 on the module installed in slot 4 of the chassis.
Maximum Allowed	Displays the maximum number of connections allowed by current device firmware.
Current Configured	Displays the number of Permanent Virtual Circuits, or PVCs, currently configured.



For some 7A06 firmware versions, Connection Data will not be displayed. In most cases, the maximum number of connections is 1024; all configured PVCs will be displayed in the Settings list box.

Settings

The Settings portion of the window contains a list box which displays information about each of the currently configured PVCs, as well as the fields used to configure new connections:

I/F	The device interface on which the PVC was configured. Note that interfaces installed in a 7C0x chassis are indexed following an XXXXY format, where X = the slot number in which the module containing the interface is installed, times 10,000; and Y = the physical index assigned to the port interface on the module. For example, an index of 40001 would refer to port 1 on the module installed in slot 4 of the chassis.
-----	--



For some 7A06 firmware versions, the I/F field will display a bogus value (like the “31” displayed in [Figure 6-1](#)); check the I/F field at the bottom of the window for the correct interface index values.

VPI	Displays the Virtual Path Identifier assigned to the connection; current versions of 7A06-01 firmware allow values from 0 - 3. Virtual Path Identifiers are used to group virtual connections, allowing for channel trunking between ATM switches. Each VPI can be configured to carry many different channels (designated by VCIs) between two points.
VCI	Displays the Virtual Channel Identifier assigned to the connection; allowable values are 0 - 1023 <i>for each VPI</i> . Each assigned VCI must be unique within its defined VPI: for example, you can assign a VCI of 14 as many as four times: once with a VPI of 0, once with a VPI of 1, and so on. Remember, it is the combined VPI and VCI designations assigned to a channel that creates the grouping of virtual connections.
Encapsulation Type	Displays the method used to encapsulate LAN packets on the selected circuit. Current versions of 7A06-01 firmware use 802.3 VC-based multiplexing for bridging protocols (designated VC MUX 802.3 Bridged); future versions will add support for ATM Forum LAN Emulation and Cabletron's SecureFast Switching. You may also see some connections assigned a type of “other”; these are default connections that cannot be modified or deleted.

Status	Displays the current administrative status of the connection: enabled or disabled. In current versions of firmware, all connections are enabled by default, and cannot be disabled.
UpTime	The length of time the selected connection has been enabled.

Add

Selecting the **Add** button either adds a new connection or modifies an existing one, using the parameters entered in the fields below the list box. A confirmation window will appear for both additions and modifications.

Delete

Selecting the **Delete** button deletes the selected connection; a confirmation window requires that you confirm the deletion.

Refresh

Selecting **Refresh** refreshes the connection information displayed in the window.

Configuring Connections

Adding a New Connection

To configure new Permanent Virtual Circuits (PVCs), enter the following information in the text fields which appear just below the connections list box:

1. In the **I/F** text box, click on the down-arrow to the right of the text field, and drag down to select the interface for which you wish to configure a connection. All available ATM interfaces will be listed in this menu; note that interfaces installed in a 7C0x chassis are indexed following an XXXXY format, where X = the slot number in which the module containing the interface is installed, times 10,000, and Y = the physical index assigned to the port interface on the module. For example, an index of 40001 would refer to port 1 on the module installed in slot 4 of the chassis.
2. In the **VPI** text box, enter the Virtual Path Identifier you wish to assign to this connection. Allowable values are 0 to 3; remember, the VPI you assign will be used to group virtual connections, allowing for channel trunking between ATM switches.
3. In the **VCI** text box, enter the Virtual Channel Identifier you wish to assign to this connection. Allowable values are 0 to 1023 *for each VPI*. For example, you could assign the same channel identifier — say, 25 — as many as four times: once with a VPI of 0, once with a VPI of 1, and so on. Again, remember that it is the combination of VPI and VCI that will be used to direct cells through the intermediate switches between the source and destination.

4. In the **Encapsulation Type** field, click on the down arrow located to the right of the field, and drag down to select the desired encapsulation type. Current versions of 7A06-01 firmware use 802.3 VC-based multiplexing for bridging protocols (designated VC MUX 802.3 Bridged); future versions will add support for additional encapsulation methods.



Selecting any of the other encapsulation types listed in the field's menu will cause a "Set Failed" error when you attempt to add the new connection.

5. Click **Add** to add the new permanent circuit to the ATM interface. The circuit is automatically enabled, and will remain in place until it is manually removed.

Deleting a Connection

To delete an existing PVC:

1. In the connections list box, click to select the connection you wish to delete.
2. Click on **Delete**. A confirmation window will appear, listing the parameters assigned to the connection and asking you to verify that you wish to delete it. Click on **OK** to proceed with the deletion, or on **Cancel** to cancel.

Symbols

% Load 3-3
% of Tot. Errors 3-4

Numerics

7C0x SmartSwitch family 1-1
 7C03 MMAC SmartSwitch 1-1
 7C04 Workgroup SmartSwitch 1-1
 7C04-R Workgroup SmartSwitch 1-1
 NIM modules 1-2

A

Absolute Value 4-2, 4-12, 4-18, 5-11
Accessing The Rmon Alarm/event List 4-10
Accessing The Statistics Window 3-1
Accum 3-6
Actions MIB 4-22
Address Mode 5-9
Admin/Link 2-10, 2-11
Advanced Alarms 4-2
Alarm Instance (RMON) 4-16
Alarm
 advanced 4-2
 basic 4-1
 log 4-5
 status (RMON) 4-12
 threshold (RMON) 4-1
Alarms and Events 4-1
Alarms Watch (RMON) 4-11
ATM 6-1
Auto-negotiation 2-24

B

Basic Alarms 4-1
Board Menus 2-9
Boot Prom, Revision 2-5
Bridge 2-10
 mapping 2-10, 2-11
 status mode 2-10
Broadcast/Multicast 4-4

Buffer Space 2-19, 3-8
Bytes 3-3

C

Cabletron Systems Global Call Center 1-8
Cancel Button 1-7
Channel Trunking 6-3
Chassis Front Panel 2-1
Claim Token Process 5-4
CMT 5-1, 5-5
Collisions 3-4
Color Codes 2-12
Color-coded Port Display 2-2
Command Buttons 1-7
Community Names 4-7
 in traps 4-7
Concentrator
 configuration window 5-2
 M Ports 5-5
 non-M Ports 5-5
 performance window 5-11
Connection
 management 5-1, 5-5
 policy window 5-6
 rules 5-7
 status 2-4
CRC/Alignment 3-4
Creating And Editing An RMON Alarm 4-13
Creating And Editing An RMON Event 4-19
Cumulative 5-11

D

Deleting An RMON Alarm, Event, Or
 Action 4-25
Delta 3-6, 5-11
 value 3-3, 4-2, 4-5, 4-7, 4-8, 4-12, 4-18
Detect 5-3
Device
 date 2-32
 menu 2-6
Device (cont'd)

- name 1-5
- time 2-32
- type 2-14
- Directed 5-4
- Discarded packets 2-19, 3-8
- Drop Events 3-3
- Dual-homing 5-7
- Duplex Mode 2-24

E

- Encapsulation Type 6-3
- Event (RMON) 4-1
- Event Index 4-12
- Event Log (RMON) 4-13
- Event Type (RMON) 4-22
- Events Watch 4-11, 4-12

F

- Falling
 - action 4-5, 4-8
 - alarm threshold 4-1, 4-2
 - threshold 4-5, 4-6, 4-8, 4-12, 4-18
- FallingEventIndex 4-18
- FallingThreshold 4-18
- FDDI connection rules 5-7
- fInNUcast 4-4
- Firmware, Revision 2-5
- Fragments 3-4
- Frame Errors 5-12
- Frame Size (Bytes) Packets 3-5
- Freeze Stats 3-6

G

- GETTING HELP 1-7
- Global Call Center 1-8
- Grouping Of Virtual Connections 6-3

H

- Help button 1-7
- Help Menu 2-8
- How Rising And Falling (RMON) Thresholds Work 4-26
- Hysteresis 4-10, 4-26

I

- I/F Summary
 - interface performance statistics 2-16
 - window 2-15
- IF Number 4-4
- IF Type 4-5
- ifInErrors 4-4
- ifInOctets 4-4
- Interface
 - detail window 2-18
 - statistics window 2-18
- IP address 1-5, 2-4
- Isolated 5-3

J

- Jabbers 3-4

K

- Kilobits 4-4

L

- Load 2-17
- Location 1-5
- Log Events (RMON) 4-22
- Log/Trap 4-5
- Logical Status 2-16
- Lost Frames 5-12

M

- MAC
 - address 1-5, 2-4
 - path 5-5
 - state 5-3
- Master (M) port 5-5
- Menu Structure 2-5
- MIB Components 2-12
- MIB II Variables 4-4
- MIBTree 4-15, 4-24
- Module Type 2-14
- Mouse Usage 1-6
- Multicast (Non-Unicast) 2-19

N

- Node Class 5-10
- Non-Op 5-3
- Non-Op-Dup 5-3
- Non-Unicast (Multicast) 2-19, 3-8

Not Available 5-3
Number of MACs 5-5
Number of Nodes 5-9

O

OFF 2-11
OK button 1-7
ON 2-11
Oversized 3-4
Owner (RMON) 4-14, 4-21

P

Packet Capture
 events 4-1
Packet 3-3
 received 2-19, 3-8
 transmitted 2-20, 3-9
 type 3-3
Peak Values 3-3, 3-4, 3-5, 3-6
Permanent Virtual Circuits (PVCs) 6-1
Physical Status 2-16
Polling Interval 4-5
Port
 display, color codes 2-2
 menus 2-9
 number 4-4
 status 2-4
 color codes 2-12
 menu 2-7
 views 2-10
Problems 3-4

R

Rate 2-17
Raw Counts 2-16
Receive Frames 5-12
Requested Target Token Rotation Time 5-4
Ring
 configuration 5-6
 management 5-1
Ring-Op 5-3, 5-12
Ring-Op-Dup 5-3
rising action 4-5, 4-7
rising threshold 4-1, 4-2, 4-5, 4-6, 4-7, 4-12, 4-18
RisingEventIndex 4-18
RisingThreshold 4-18
RMON alarm description 4-26
RMT 5-1

S

Sample Type 4-18
SecureFast Switching 1-2
Selecting Port Status Views 2-10
Set Button 1-7
Setting An RMON Alarm Variable 4-15, 4-24
SMT Connection Policy 5-6
SMT Version 5-4
Startup Alarm 4-18
Station List 5-9
Statistics (RMON)
 Ethernet 3-2
Status (alarm) 4-5
Switched Virtual Circuits (SVCs) 6-1

T

Technical Support 1-8
Threshold Pairs 4-27
T-Neg. 5-5
To Change The Status View Of Your Ports 2-10
Topology 5-10
Total 3-6
 errors 4-4
Trace 5-4
Traditional Switching (or bridging) 1-2
Transmit Frames 5-12
Transmit Queue Size 2-19, 3-8
Trap (RMON) 4-22
T-Req. 5-4
Troubleshooting 2-19
Twisted Ring 5-7

U

Undersized 3-4
Unicast 2-19, 3-8
Unknown Protocol 2-19, 3-8
Up Time 2-4, 2-15
Upstream Neighbor 5-10
Utilities Menu 2-8

V

VC MUX 802.3 Bridging 6-3, 6-5
viewing an RMON event log 4-25
Virtual Channel Identifier (VCI) 6-3
Virtual Path Identifier (VPI) 6-3

W

Wrapped Ring 5-7

